koat

Breaking Down Silos
AI-Powered Intelligence to Secure LA

Presented by:

Connor Ross, President/Co-Founder, Koat.ai
Dallas Toth, CEO/Technical Founder, Koat.ai

Be Ready.

Today

Why AI and information security operations improvement matters now more than ever.

- Our story
- Disinformation & the threat landscape
- Public safety in the AI era
- AI in Action: LA Case Study
- Key takeaways for your teams & CTA

The Problem

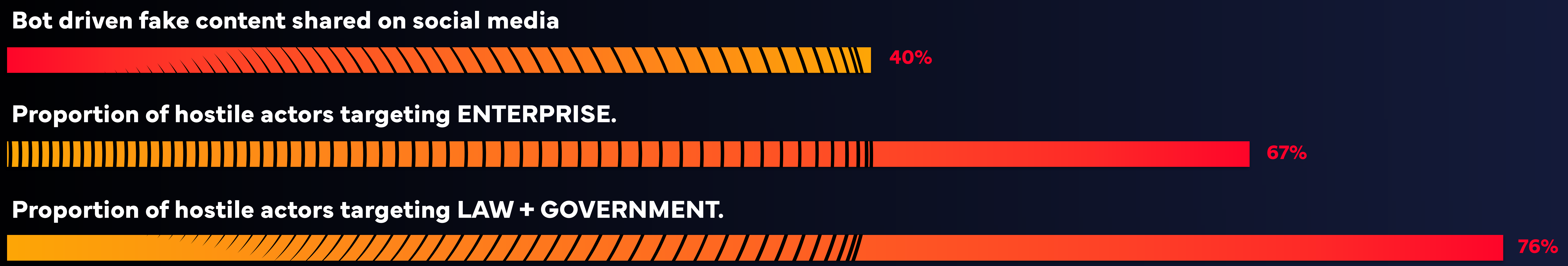
The Threat of Disinformation and the Data Deluge

Disinformation & Synthetic AI is accelerating.
37% of all web traffic is coming from malicious bots.

Security leaders are overwhelmed and need clarity. Trust is eroding.
Only 32% of Americans trust news media, and fake news costs the global economy $78 billion annually.

Your team is losing time.
64% of SOC analysts report that manual work consumes more than half of their time.

THE PROBLEM IN THE DATA



Koat automates

90%

of open-source data collection & triage.

Koat improves operational efficiency, enhances digital risk detection, and enables more responsive, data-informed decision-making.

- Surfaces open-source and disinformation threats
- Delivers real-time alerts, anomaly detection & media analysis
- Uses GenAI to contextualize narratives and generate intel
- Visualizes risk across dashboards, APIs & Scout (our GenAI analyst)
- AI Workflow Integration: Custom templates, procedures, and output formats

We gather the data that is important to you, 20,000 + RSS Feeds (ie. CNN, Financial Times, Wall Street Journal) as well as:

We turn fragmented data into **fast, trustworthy threat intelligence** that helps you act faster and with more clarity.

Intelligence Dashboards

Real-time media & sentiment monitoring, disinformation, narrative detection, foreign influence.

Scout Auto-Insight

GenAI tool for reporting, summarizing, and analysis.

Data Integrity Layer

Raw data + context + trust.

Reports, Signals & Anomalies

Trends, amplification, coordinated content.

Integrations & APIs

Served into your environment.

AI First Infrastructure with Source Verification

Trust but verify AI predictions with full raw source verification.

Our Story

2010- 2021

Bot Farms & (Harmless) Influencer Harvesting

The Spark

Real Impact of Disinformation Brought Home

2021 - Present

Proactive Threat Intelligence to Deliver Truth, Trust and Transparency

Our mission to bring trust, transparency and clarity of data in a world filled with manipulation.

A Brief History of

Disinformation and Fake Accounts

Early 2000's / The inception of Fake Accounts

The 2010's / The Social Media Boom

Covid-19 Milestone

Present Day / AI-Driven Misinformation

Public

Erosion of Trust

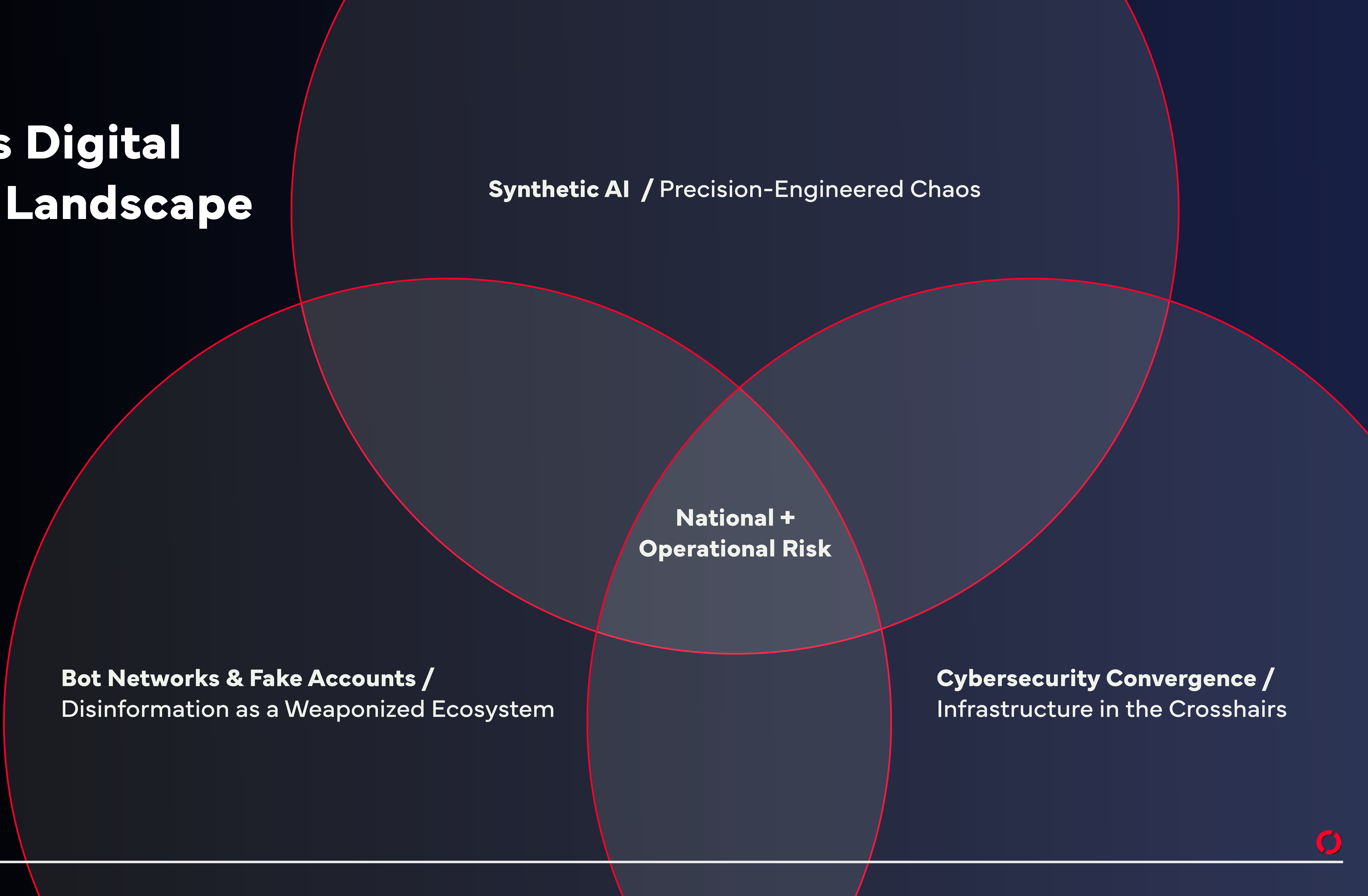
Enterprise

Corporate Disinformation

Government

Threat to Democracy

Today’s Digital Threat Landscape



Synthetic AI / Precision-Engineered Chaos

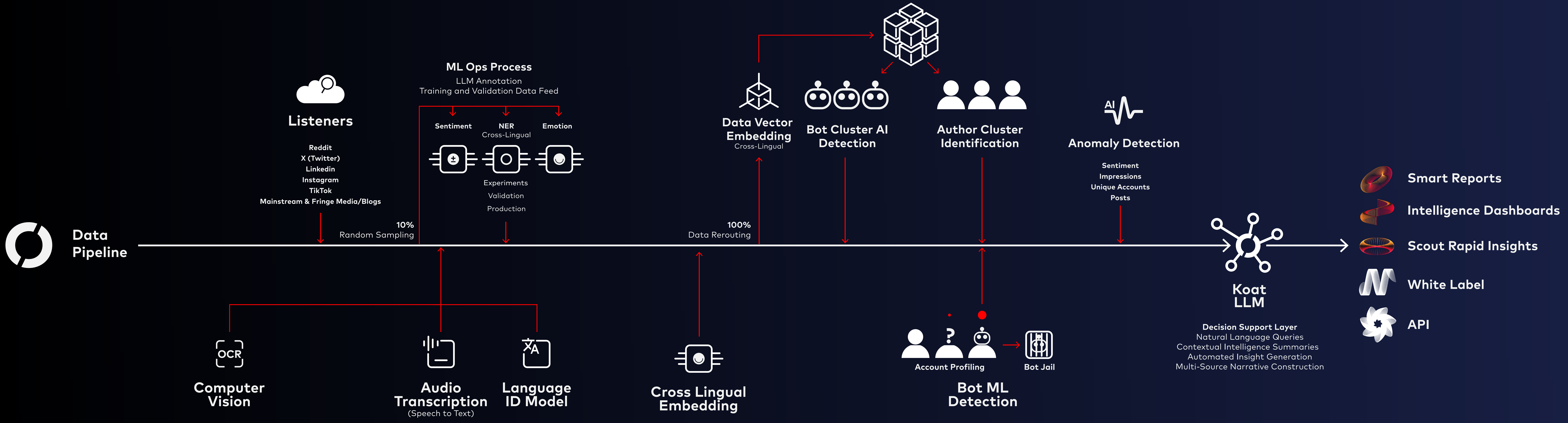
Bot Networks & Fake Accounts /
Disinformation as a Weaponized Ecosystem

Cybersecurity Convergence /
Infrastructure in the Crosshairs

National + Operational Risk

Why AI-infrastructure is Critical for Public Safety

- Timely, relevant, actionable intelligence
- Unified Intelligence & Knowledge Mobilization
- Efficiency, Automation, and Cost Savings
- Proactive threat intelligence in evolving threat landscape



Data Pipeline

Listeners

Reddit
X (Twitter)
Linkedin
Instagram
TikTok
Mainstream & Fringe Media/Blogs

10%
Random Sampling

ML Ops Process
LLM Annotation
Training and Validation Data Feed

Sentiment

NER
Cross-Lingual

Emotion

Experiments
Validation
Production

Computer Vision

Audio Transcription
(Speech to Text)

Language ID Model

100%
Data Rerouting

Cross Lingual Embedding

Data Vector Embedding
Cross-Lingual

Bot Cluster AI Detection

Author Cluster Identification

Account Profiling

Bot Jail

Bot ML Detection

Anomaly Detection

Sentiment
Impressions
Unique Accounts
Posts

Koat LLM

Decision Support Layer
Natural Language Queries
Contextual Intelligence Summaries
Automated Insight Generation
Multi-Source Narrative Construction

Smart Reports

Intelligence Dashboards

Scout Rapid Insights

White Label

API

AI in Action

Case Study

AI in Action - Case Study

Methodology: Operational Use of LLM Prompts for Social Media Intelligence, Attribution, and Narrative Manipulation Detection

Scalable, repeatable best-practice approach for leveraging Large Language Models (LLMs) to extract tactical and strategic intelligence from social media during civil unrest and politically sensitive events.

Briefing and intelligence in Real-Time.

1. **Data Collection & Cleaning**
2. **Narrative & Threat Detection**
3. **Disinformation & Manipulation Analysis**
4. **Attribution & Actor Mapping**
5. **Structured Output & Visualization**
6. **Reporting & Alerts**

Step 1

Data Collection & Cleaning

Objectives /

Collect protest-related social media, clean + enrich it for analysis.

Koat ingested 100s of thousands of posts across traditional and social media relating to conversations and threat vectors surrounding the LAPD, LA Riots, Los Angeles, LA28

Number of Posts / **214,0416**

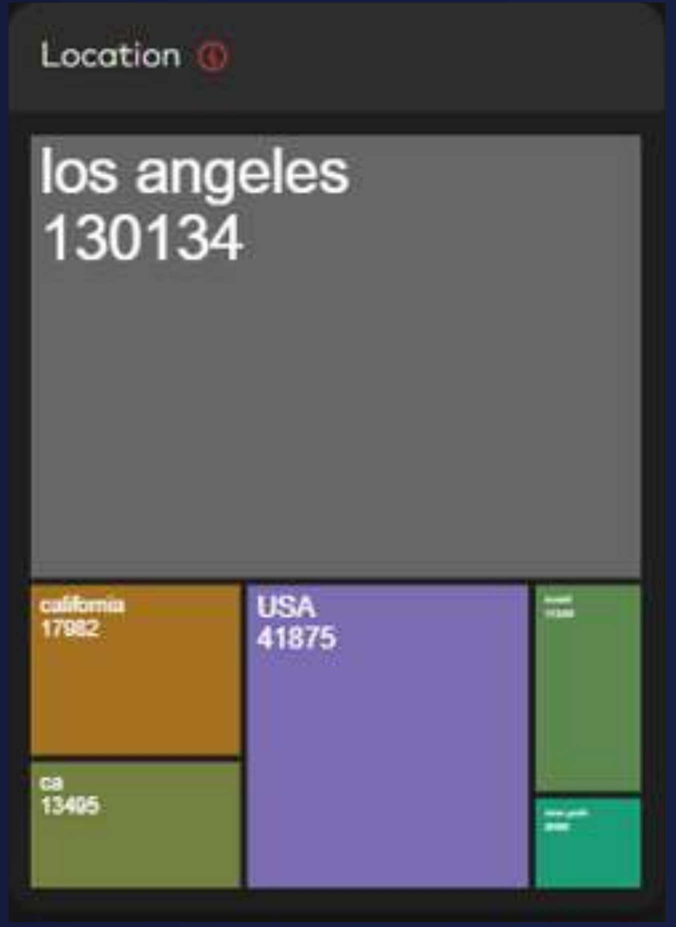
Unique Authors / **76,403**

Public Sentiment / **-31.1**

Total Impressions / **149,380,494,041**

Manipulator Sentiment / **-22.4**

Manipulator Impressions / **26.86%**



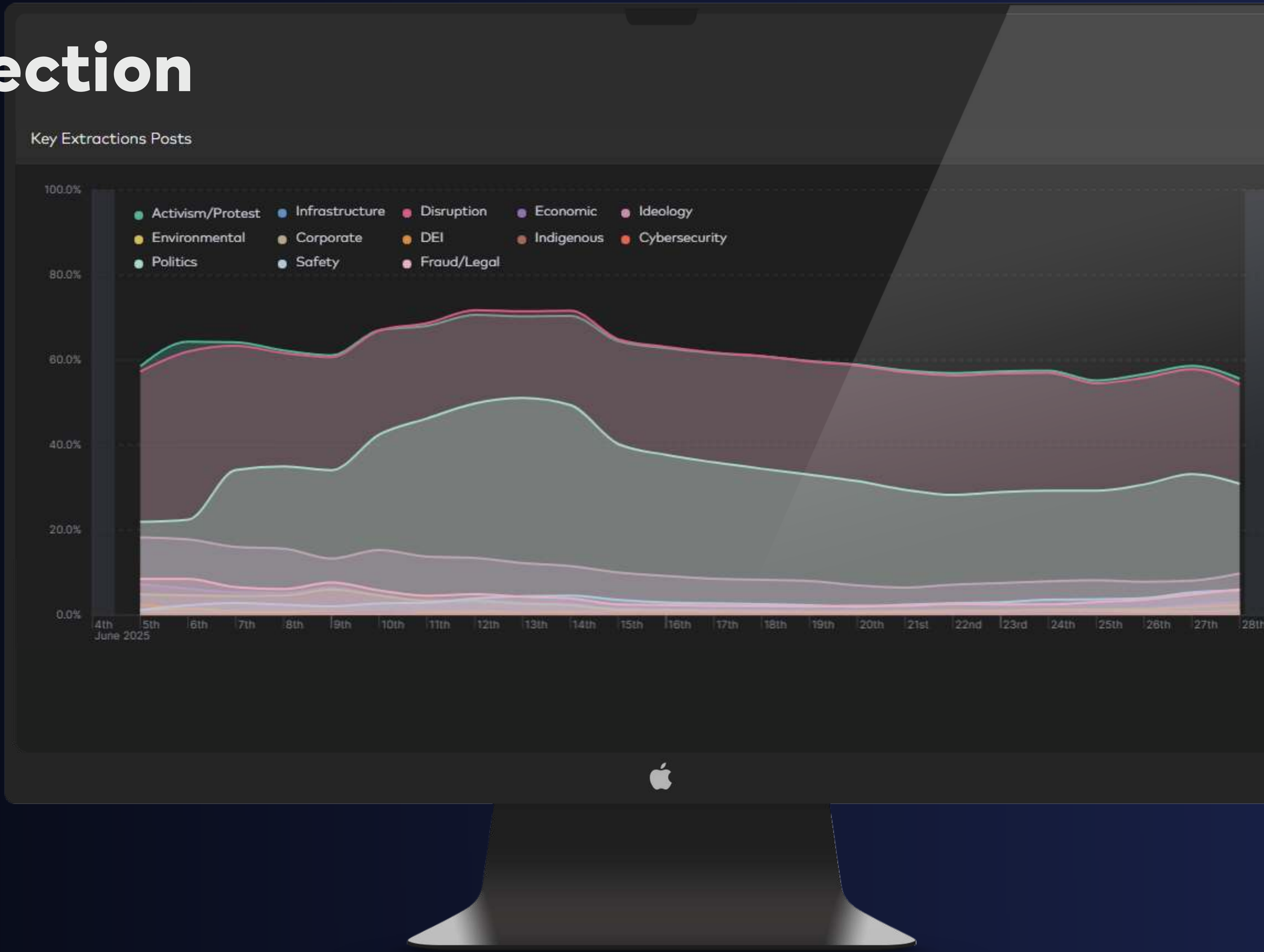
We gather the data from 20,000 + RSS Feeds (ie. CNN, Financial Times, Wall Street Journal) as well as:

Step 2

Narrative & Threat Detection

Objectives / Identify themes, groups, flashpoints, calls to violence, early warnings.

- Run narrative discovery
- Detect intent to escalate
- Identify activist groups, influencers
- Generate tactical alerts and safety warnings



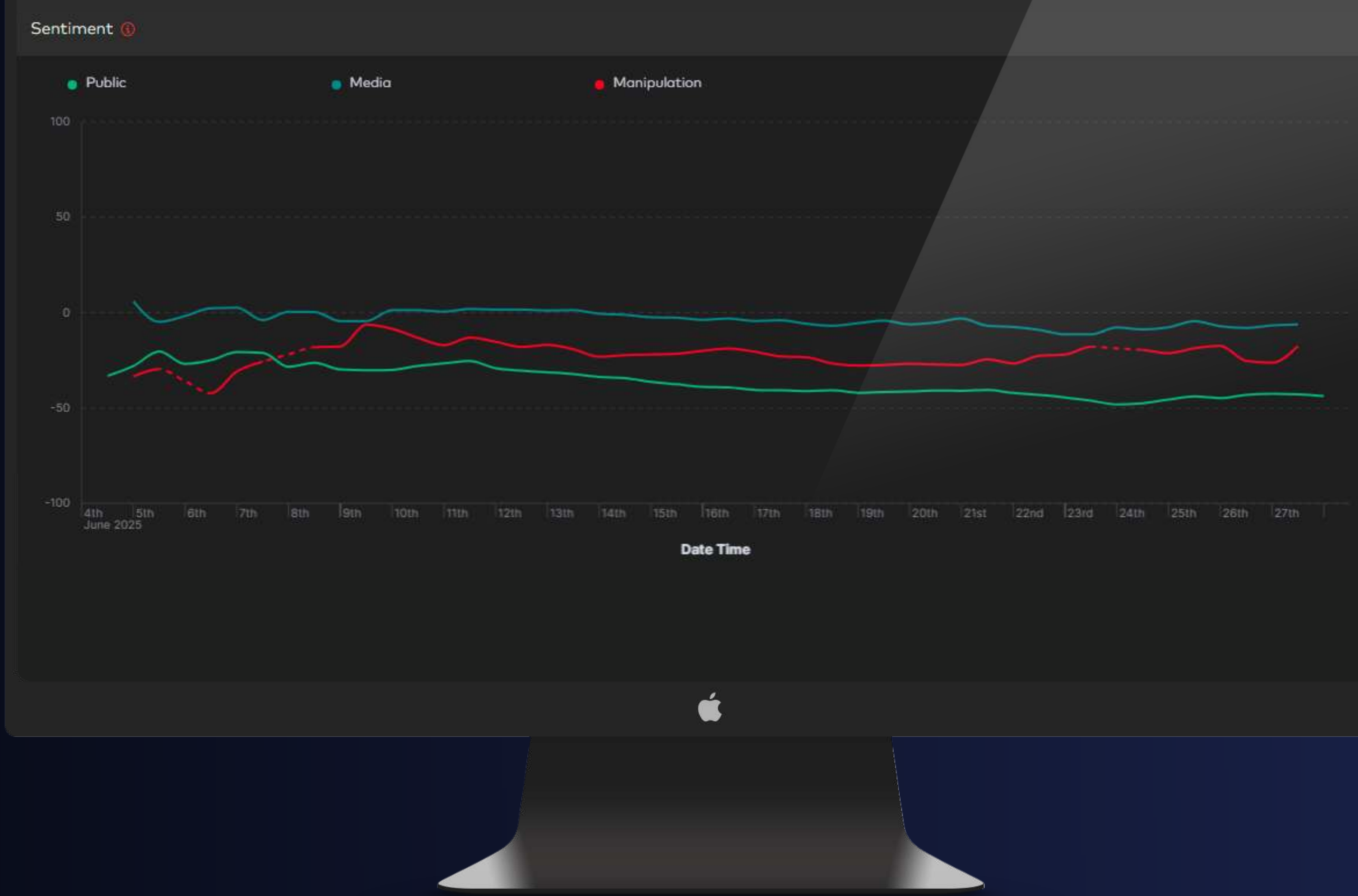
Be Ready.

Step 3

Disinformation & Manipulation Analysis

Objectives / Detect and map PSYOPs, botnets, sockpuppets, influence injection

- Run manipulation signature prompts
- Apply enhancements: bot score, geo-mapping, authenticity classification
- Detect early narrative seeding and media manipulation

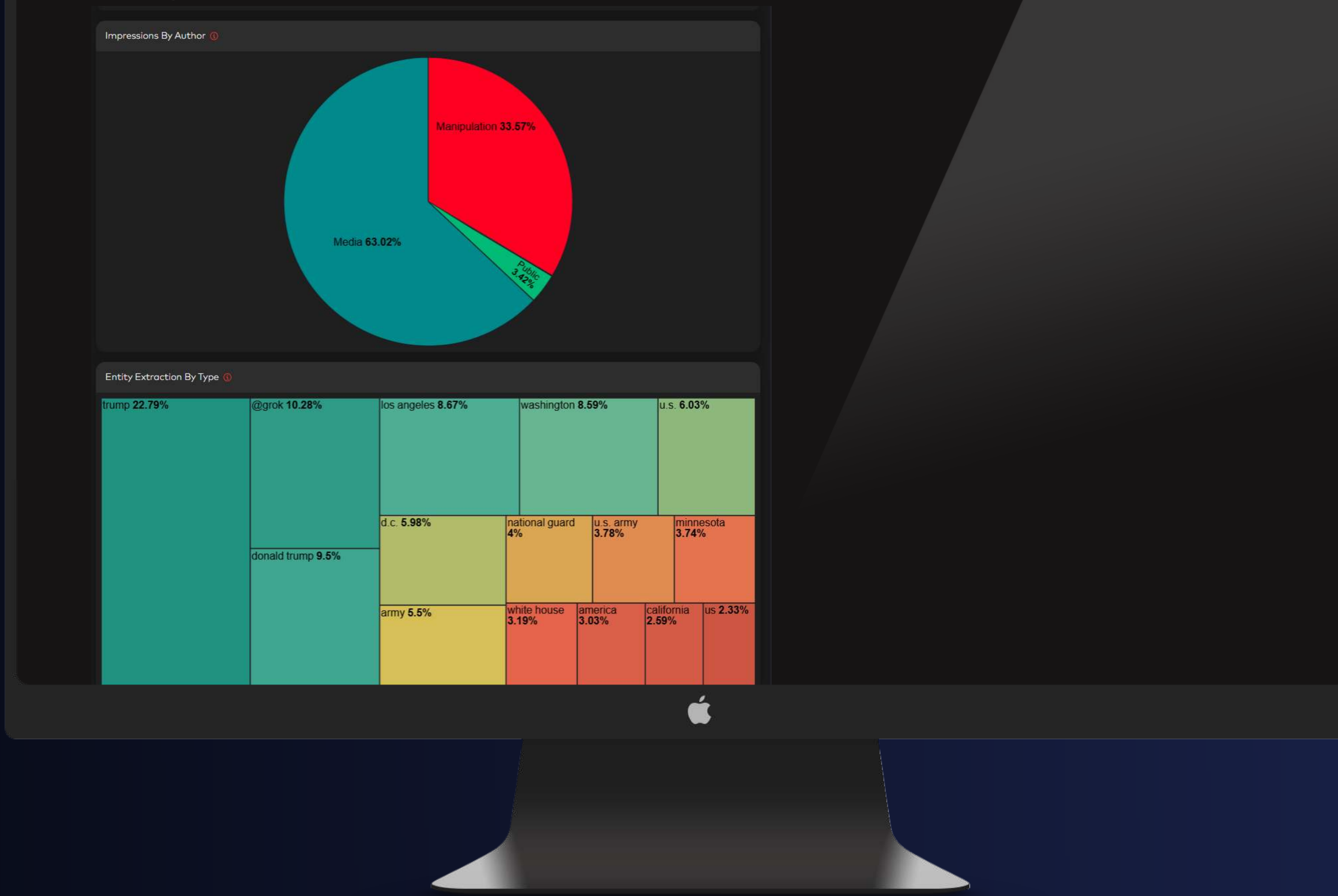


Step 4

Attribution & Actor Mapping

Objectives / Classify users, build profiles for future monitoring, and enable network discovery

- Agency-style prompts:
  - SIGINT/HUMINT cues
  - Find affiliations, actors driving emotion
  - Group mapping of instigators vs. amplifiers
  - Create persistent monitoring profiles

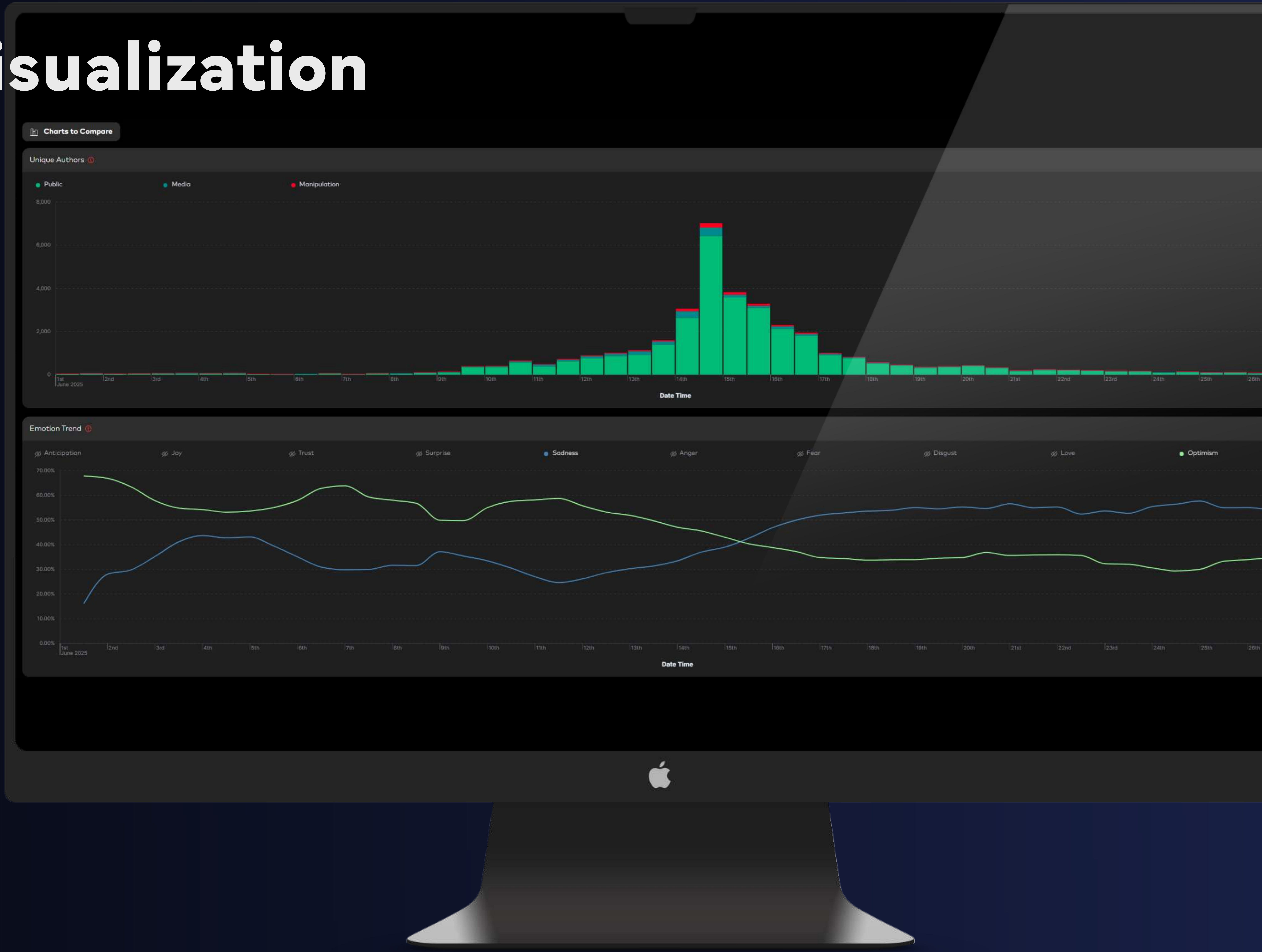


Step 5

Structured Output & Visualization

Objectives / Convert LLM outputs into structured formats for tooling (e.g., Maltego, Elastic, MISP)

- Parse LLM output into structured JSON/ YAML
- Output to dashboards
- Import structured actors/entities
- Connect external OSINT enrichments



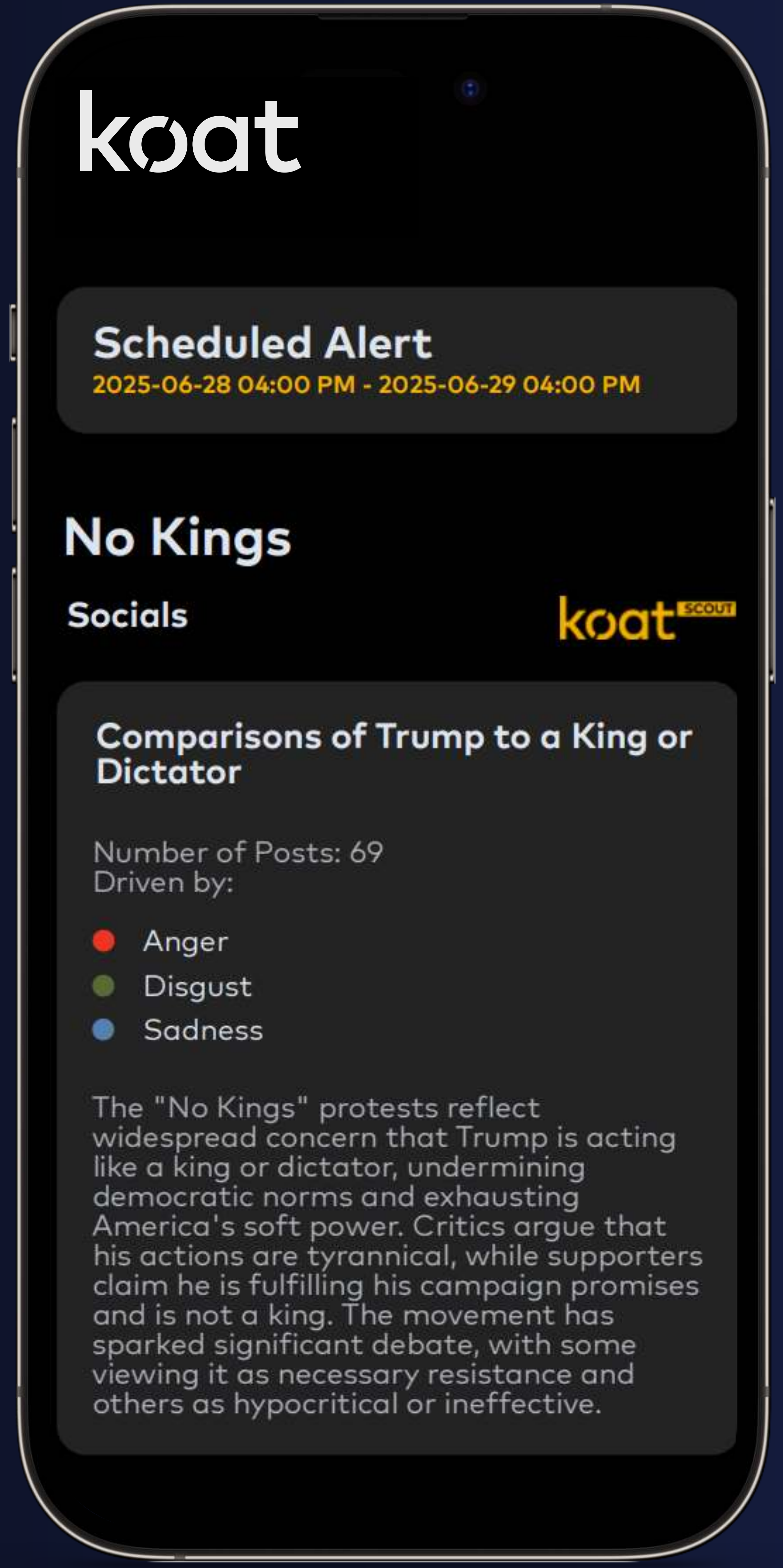
Be Ready.

Step 6

Reporting & Alerts

Objectives / Communicate intelligence to LE, public safety, fusion centers

- Auto-generate protest narrative briefings
- Send watchlist alerts (escalation, threats, doxing
- Actionable outputs:
  - Geo-specific briefings for patrol
  - Top influencers to watch
  - Channels spreading harmful narratives



koat

Scheduled Alert
2025-06-28 04:00 PM - 2025-06-29 04:00 PM

No Kings

Socials

koat SCOUT

Comparisons of Trump to a King or Dictator

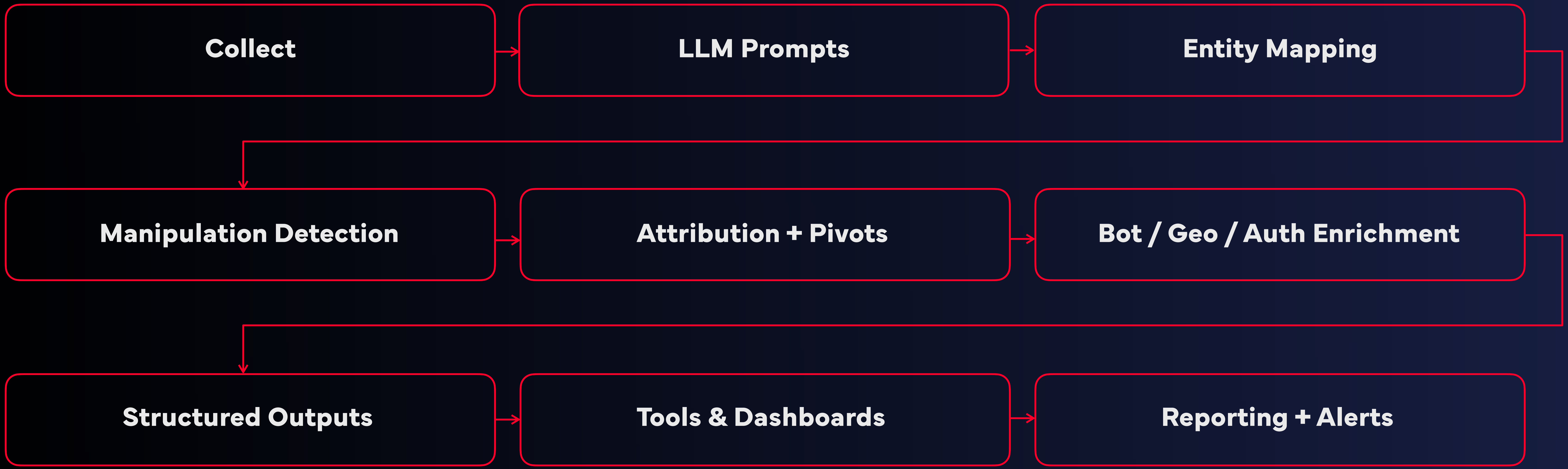
Number of Posts: 69
Driven by:

● Anger
● Disgust
● Sadness

The "No Kings" protests reflect widespread concern that Trump is acting like a king or dictator, undermining democratic norms and exhausting America's soft power. Critics argue that his actions are tyrannical, while supporters claim he is fulfilling his campaign promises and is not a king. The movement has sparked significant debate, with some viewing it as necessary resistance and others as hypocritical or ineffective.

End-to-End

Intelligence Flow



Collect

LLM Prompts

Entity Mapping

Manipulation Detection

Attribution + Pivots

Bot / Geo / Auth Enrichment

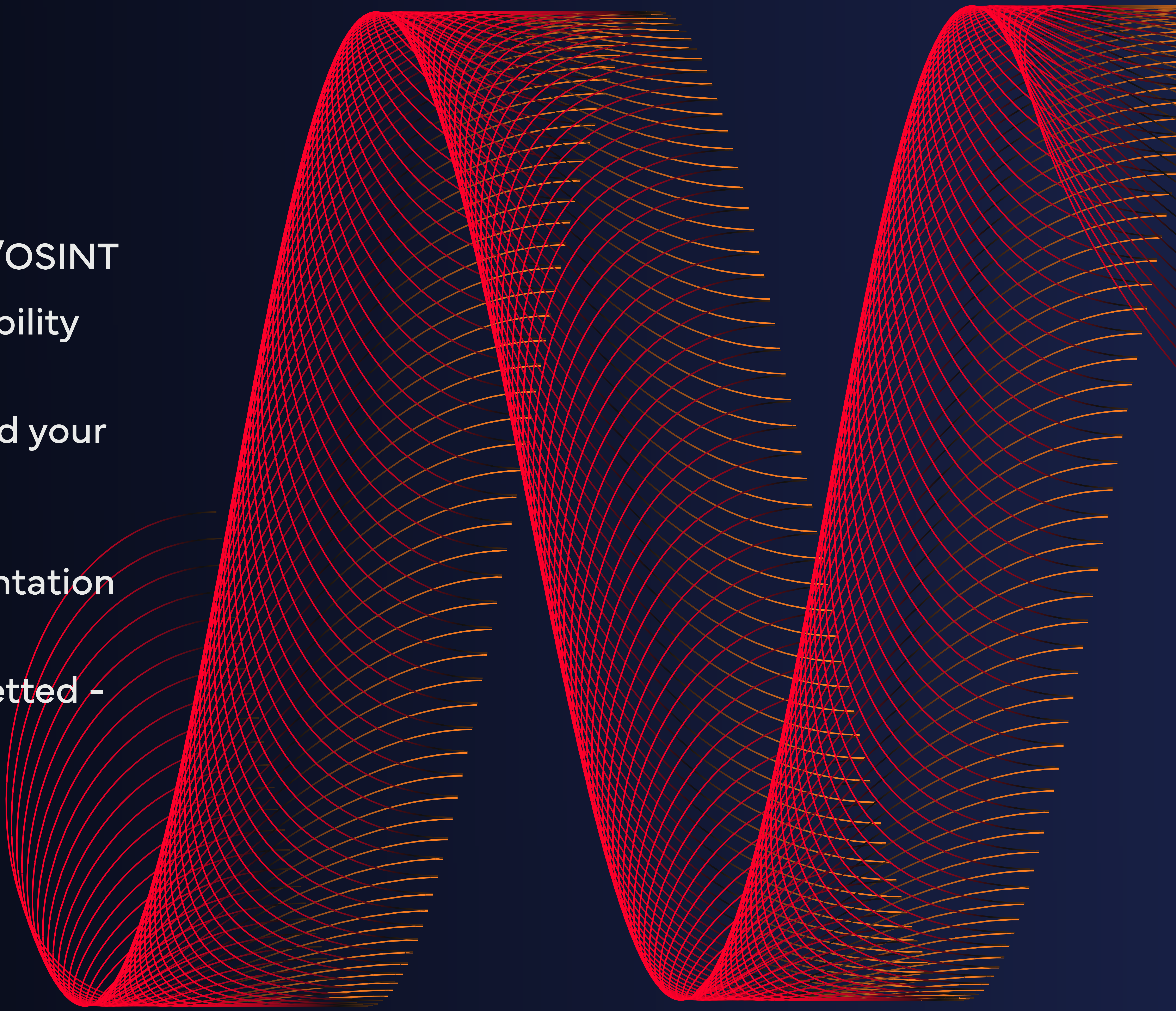
Structured Outputs

Tools & Dashboards

Reporting + Alerts

Lessons Learned

- Importance of timely, relevant, actionable PAI/OSINT
- Prompting and discovery simplicity with the ability to be tactical and strategic
- Collect the information that matters to you and your workflow, eliminate noise
- Have the ability to prioritize threats and opportunities - human in the loop and augmentation - last mile delivery
- Forensic methodology on top of data that is vetted - triggers, signals



Why This Matters

The New Age Of Information Warfare is here.

A Glimpse of the Future

Emerging Threats to Watch, such as AI-generated disinformation, deepfakes.

AI-native solutions and real-time OSINT (Open Source Intelligence).

Call to Action

We Must Act Together.

Collaboration is Key.

Invest in Tools and Solutions.

Thank You

Connor Ross
Co-Founder, Koat.ai

connor@koat.ai
linkedin.com/in/cmross1/