The Oregon Secretary of State (SoS) – MDM (Misinformation, Disinformation, and Mal-information) Analysis Platform Service

Solicitation #S-16500-00002374

Mis, dis and Mal-information undermines public confidence in the electoral process and ultimately trust in the democratic system. At Logically, we understand the tremendous effort put forth to protect U.S. elections by state and local officials to protect the sanctity of the vote. Logically hopes to provide the Secretary of State (SoS) with state of the art technology and expertise to enhance the SoS's vital mission. **The Logically LTD, an Oregon registered business, thanks you for the opportunity to submit our proposal in support of your mission and this solicitation.**

Section One: – Overview & Understanding of MDM

Who We Are.

Logically is a technology company combining advanced artificial intelligence with human expertise to tackle harmful and problematic online content at scale. It aims to provide everyone, from individual citizens to national governments, with the tools to identify and disarm damaging and misleading information. Logically is an award-winning international team of over 190 data scientists, engineers, analysts, developers, and investigators, united by the company's mission to enhance civic discourse, protect democratic debate and process, provide access to trustworthy information and prevent violence to people and property . Established in 2017, Logically has offices in the U.S., India, and the United Kingdom.

What Logically does.

Logically has developed a suite of products and services to immediately identify threats of violence and to analyze the harm caused by the spread of MDM. These include Logically Intelligence (LI), Logically's sophisticated threat intelligence platform.

In addition, Logically's dedicated investigative and fact-checking teams produce detailed analyses and reports on specific MDM actors and trends. Logically has produced numerous deep-dive investigations which have enabled governments to make time sensitive critical decisions.

Logically's combination of artificial and human intelligence means it can apply both scale and nuance to the problem of MDM, identifying issues before they become widespread.

Logically Intelligence.

The LI platform provides at-scale analysis, classification, and detection to help partners monitor the online media landscape. The platform quickly identifies the spread of damaging narratives that undermine confidence in the electoral process and may lead to real-world harm. Additionally, LI includes a suite of countermeasures, or actions that clients or users can take in response to MDM. LI is one of the only platforms to integrate analytical capabilities and countermeasure deployment to tackle MDM.

The platform is primarily designed for governments and public sector entities concerned about the impact of MDM on democratic processes, national security, or public safety. For example, for a battleground US state in the 2020 election, Logically Intelligence ingested millions of individual pieces of content, further identifying and analyzing 40,000 threats to election integrity and public safety for review and countermeasures.

Logically specifications:

Capabilities	Logically
Advanced AI/ML capabilities	☑
Near-real time monitoring of the information environment	☑
Ingests content from over two dozen unique social media platforms and hundreds of other online sources	☑
Ability to ingest additional social media sources upon request within 2-3 days	☑
Ability to ingest and translate non-English content	☑
Automatically determine the sentiment of content across multiple languages	☑
Automatically classify violent content into a criminal, active shooter, workplace, or terrorism categories	☑
Automatically classify content as a potential threat to life or threat to property	☑
Automatically detect inauthentic activity	☑
Integrated fact-checking to determine if content could be misinformation/disinformation	☑
Automatically identify emerging narratives	☑

Capabilities	Logically
Automatically identify "patient zero" or the account that started a narrative	☑
Ability to compare narratives based on volume, threat level, and other characteristics	☑
User-generated tactical custom reports	☑
Graphic network analysis and visualization across all platforms (ex. Twitter, Facebook, message boards)	☑
Easy to use dashboard and user interface	☑
Ability for OSINT team to conduct full investigations and produce long form reports	☑
The ability for OSINT team to produce tactical reports on the frequency required by the customer.	☑
Existing 24x7 operations	☑
Ability to determine communities within an information environment (ex. anti-vaxxers)	☑
Ability to identify content, hashtags, trends, etc. within a specific community	☑
Ability to quickly determine signs of foreign influence related to a specific topic	☑

Capabilities	Logically
Built-in feature to enable users to immediately gather intelligence about the users of an account	☑
Built-in feature to enable users to push flagged content to law enforcement or social media companies	☑
Built-in workflow process to track the status of leads and reports	☑

Our Understanding

How we think about the threat.

As former national security professionals, data scientists, election experts, and mis/disinformation specialists, we understand the array of threats that will target the elections this fall and have proactively mapped out the information environment surrounding the 2022 Oregon and additional state midterm elections. Our ongoing work in the social media threat space leads us to believe that threats to election officials will come from a diverse range of actors. We continually update our software to match the ever evolving threat landscape.

Understanding What's at Stake: Logically's 2022 Election Overview.

Part of our process is to provide Oregon and the other states with an immediate notification system should inauthentic accounts appear and disseminate faulty information. This type of rapid response capability is critical in reducing the damage and impact of such incidents. Logically can also tactically in real time support the prevention of foreign adversary disinformation efforts, including those being executed via social media or media websites, or via other online sources to alter or shut down government websites. For example, a tactic that adversaries used in the 2016 and 2020 elections was replacing a .gov with a .com to make a website appear legitimate. Additionally, our platform can identify when adversaries are pushing "deep fake" content in an effort to foment social unrest, influence voter perceptions, decisions, or actions, or alter voter turnout. In other instances, rumors, conspiracy theories, and illiberal threat actors may peddle false or misleading information about

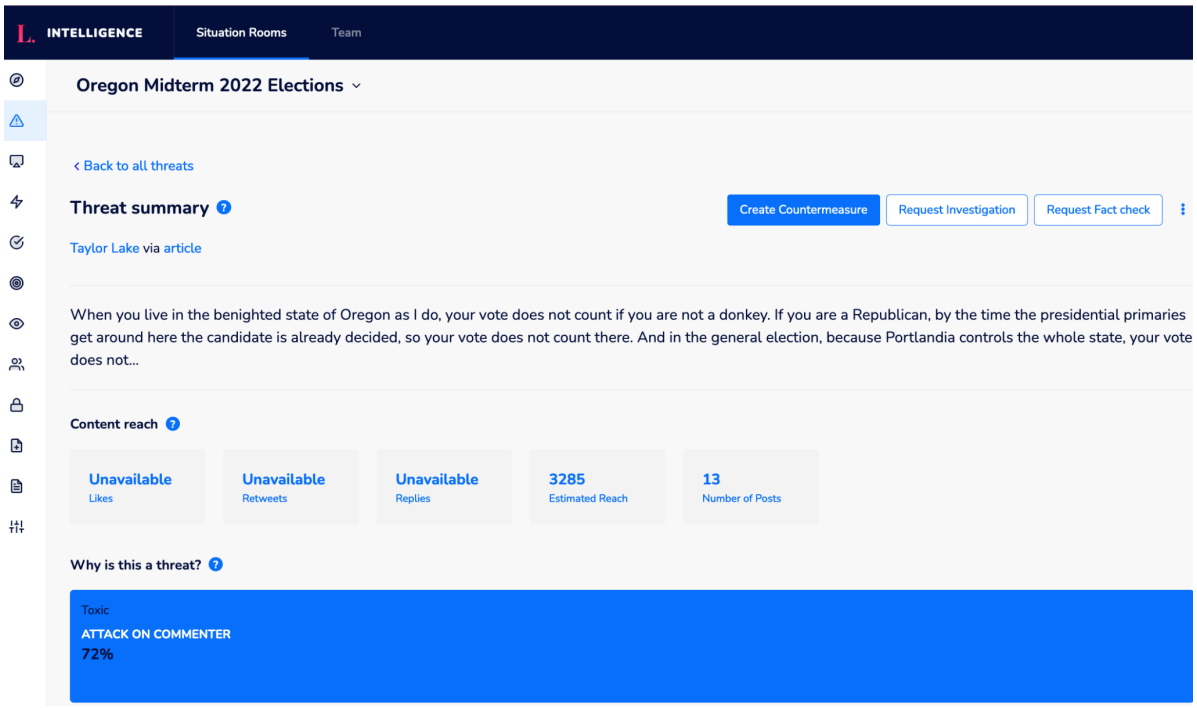
the voting process leading to unexpected problems. For example, these may include social media posts, text messages, or robocalls falsely reporting closed or changed locations of polling stations, or false physical incidents at polling stations. Logically has the capability to identify this harmful information from its source, allowingelection officials to immediately mitigate such scenarios.

Furthermore, our constant monitoring allows us to immediately identify when elections officials have been doxxed or if they have been victims of incidents such as hashtag poisoning (the creation of an abusive hashtag), which is then leveraged as a rallying cry for cyber mobs to attack an individual or SOS effort. Logically's platform identifies these trends in real time and returns the information advantage so SOS can make fast, informed decisions.

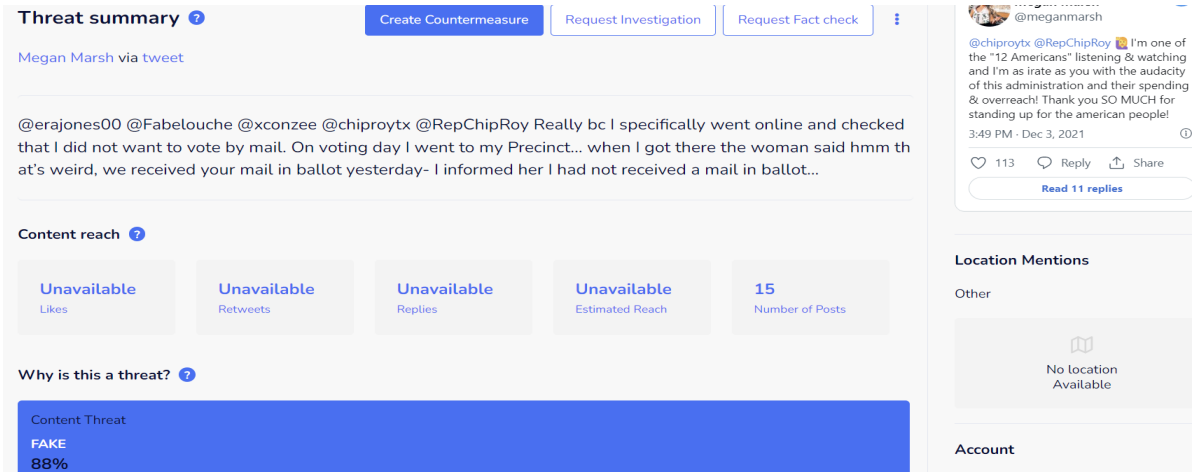
In preparation for the 2022 Oregon Elections:

We are working to combat state-specific misinformation about:

1. Who can vote

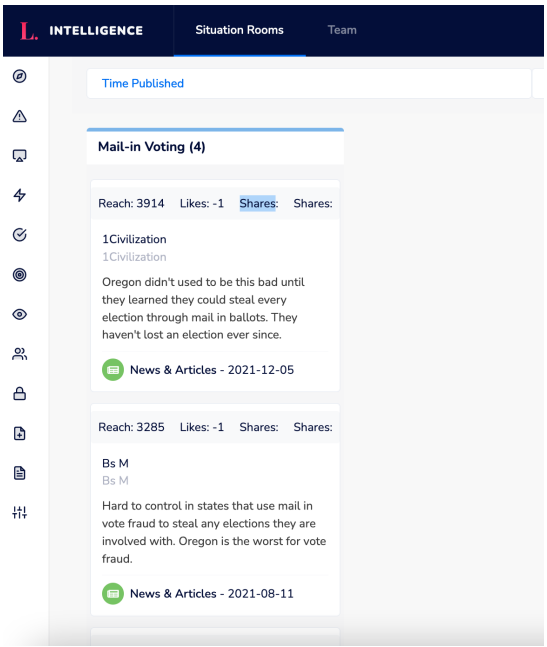


2. When voting commences.



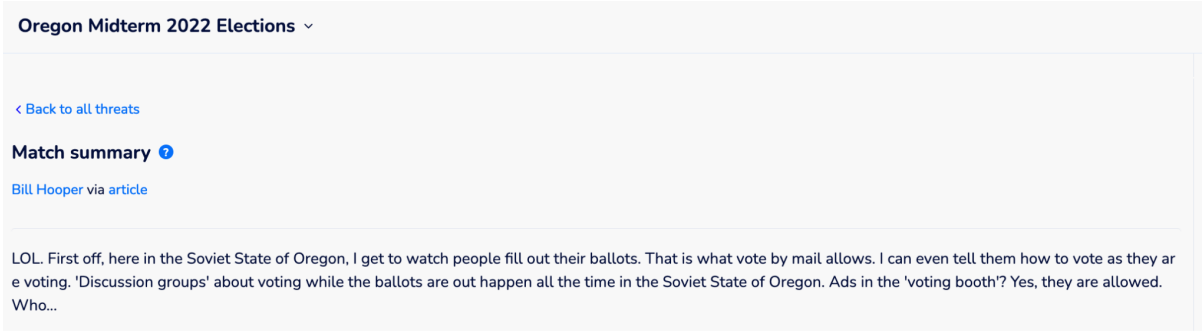
We map out the social media ecosystem and overlay it with key dates to position our clients to catch MDM narratives as early as possible. Below is a common type of false narrative designed to dissuade people from voting.

3. Where to vote



Logically can identify specific threats of MDM such as these comments about mail-in-voting that have reached over 3,000 users.

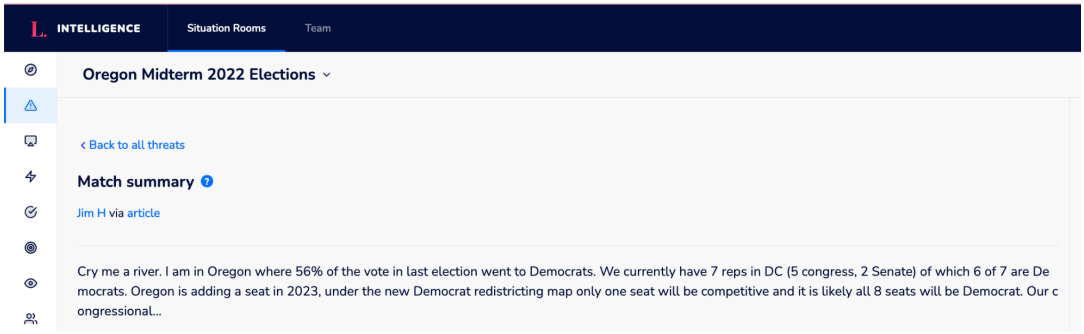
4. How to vote



5. Official election procedures

Logically's platform also allows you to interact directly with the source of the content for further analysis.

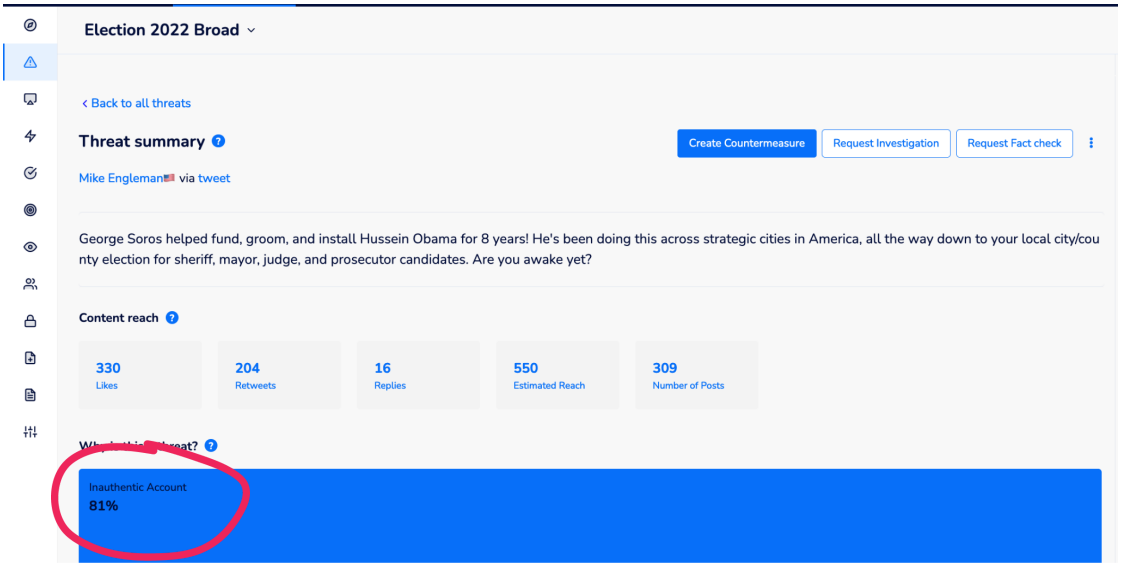
6. Updates to voting laws/redistricting communication



Identifying MDM

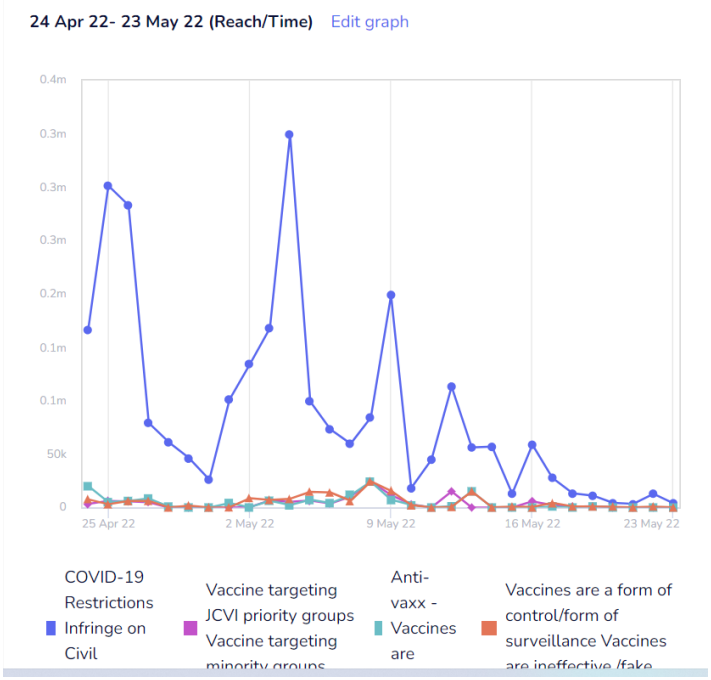
The types of disinformation techniques, tactics, and procedures states will encounter, and we are prepared to address at scale are:

1. Inauthentic account behavior.



Our tech assigns a score to determine inauthentic behavior. In the below example this content received an 81% mark.

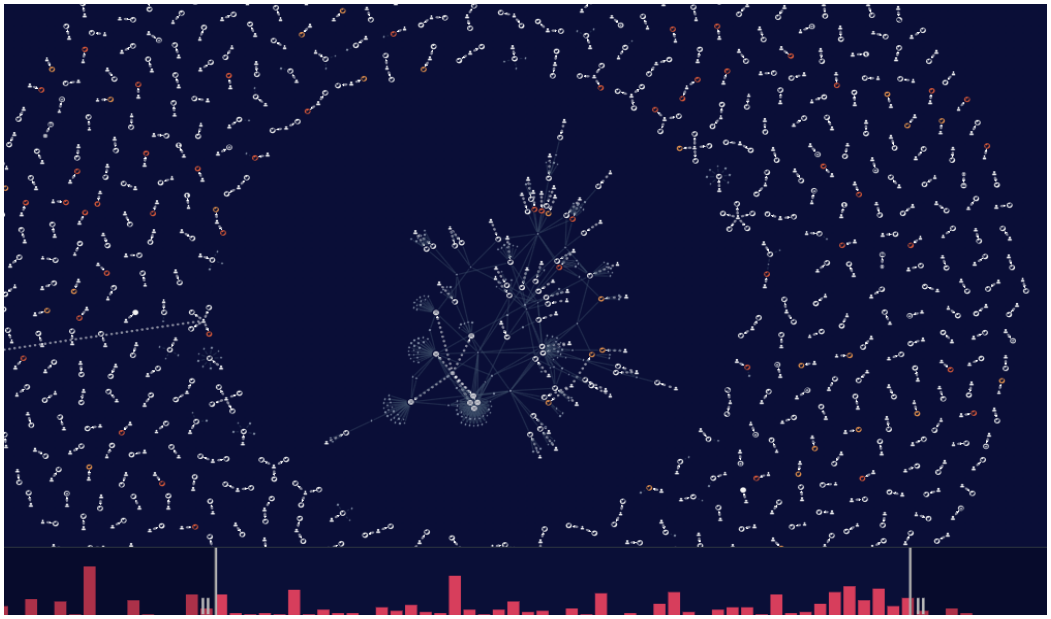
2. Coordinated messaging



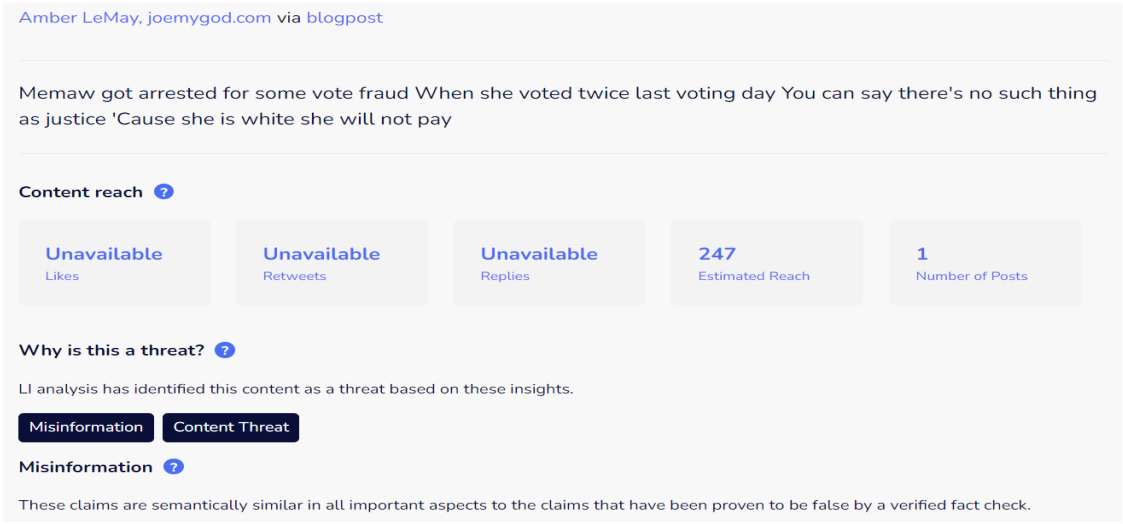
Our unique narrative monitoring enables decision makers to instantly understand the scope and scale of an MDM campaign

3. Cross platform narrative laundering

Hundreds of thousands of pieces of content are immediately displayed to demonstrate how narratives move across platforms

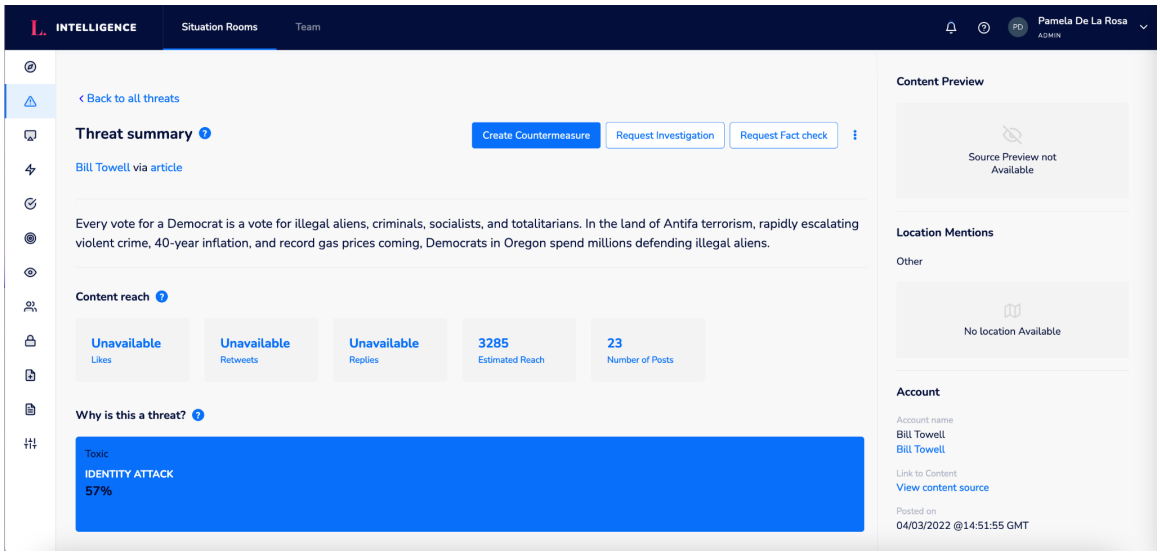


4. Polarization efforts



Posts like the one above are designed by adversaries to polarize voters

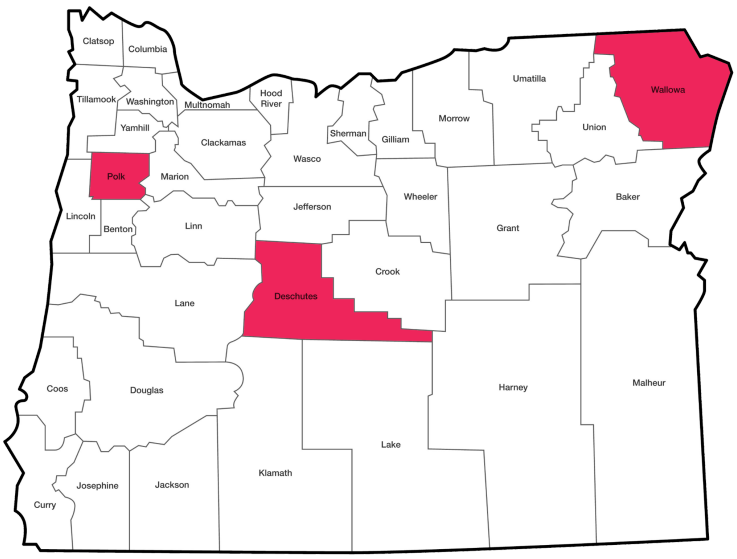
5. Content provenance determination



Not only can Logically identify various types of disinformation techniques, tactics, and procedures but we also have the capability to identify the types of threats trending on platforms.

We Start from the Local Level.

We can assist our customers in structuring keyword queries to create a monitoring capability for each county. We then continue to tailor what the room is monitoring by organizing the information into an easy to find user experience. We are already tracking threats to elections across the U.S. and have a detailed understanding of the evolving threat landscape.



Our users can also easily create their own searches and update them to meet the ever-changing real world environment. This can be used at the state and county level to meet different county-specific issues.

Our Experience

The following is a summary of recent work for clients relevant to the government and election arena:

1. **Supporting election integrity efforts during Northern Island elections during May, 2022.**
   Logically identified worked to spot MDM and assist officials to mitigate arguably one of the most contentious elections in Europe.

2. **Supporting election integrity efforts in Hungary during the country's April 2022 elections.**
   Logically worked to identify MDM narratives impacting the Hungarian 2022 election. Logically was hired by the German Marshall Fund's Alliance for Securing Democracy (ASD), which works to prevent the erosion of democracies. Logically identified 8 unique themes and over 10 specific narratives within Hungarian public discourse that were vulnerable to and/or contained potential MDM. ASD used Logically's analysis, provided via Logically Intelligence and OSINT support, in their article Key Narratives to Watch Before Sunday's Hungarian Elections – Alliance For Securing Democracy (gmfus.org)

3. **Ongoing support to a U.S. national security client.**
   Logically currently helps a U.S. national security client track and analyze hostile countries' MDM narratives targeting allied countries. Logically has configured 20 unique information environments in Logically Intelligence that span 7 countries, while also providing OSINT support.

4. **Ongoing support to a European Government for threat monitoring and VIP protection.**
   Since January 2021, Logically has been providing one of the most prominent European governments with real time threat reporting to cabinet level officials and their staff. The threats are emanating from individuals and groups who believe in COVID related conspiracies. As most of our work is classified, we can only offer broad generalities about the nature of this work.

5. **Supporting election integrity efforts in a major battleground state during the 2020 U.S. elections.**

   In 2020, many states were witnessing a serious problem with misinformation circulating on social media and within the media itself. Falsities such as long lines at voting booths and drop boxes being open to fraudulent activity were

being used as a blatant attempt at voter suppression. One major battleground state took additional steps to deliver a safe and trusted election result by choosing to work with Logically.

Logically's remit was to focus on identifying and analyzing misinformation being shared on social media and news articles that originated from the state itself, as well as surrounding states that mentioned its election, rather than focusing on the wider political landscape. This meant we were able to narrow our focus down to a very specific geographical area, delivering highly localized and actionable information.

Working with the Office of the Secretary of State, we highlighted a number of keywords that were flagged by our systems each time they were mentioned on social networks and within the media. Our AI models then classified each piece of content to determine whether it contained concerning entities, toxic information such as threats, whether it was coming from an automated account and whether that account was located outside the state. We were also able to analyze data by threat level, enabling the team to categorize the information they were seeing and prioritizing where action was urgently needed.

Furthermore, the Logically OSINT team played a crucial role in tracing harmful content back to any online instances using big data and granular investigation techniques. For example, the black community was targeted with convoluted messaging to create confusion around what identification was required to vote, ultimately deterring people from casting their ballot. To bolster this activity, the team also monitored communities such as Proud Boys and Militias for potential disruption and risks at the polling stations themselves.

With constant access to the platform, the Secretary of State's team could see what information was being surfaced by our AI and where it was originating from, enabling them to identify problematic narratives and content for which they could tailor specific counter- messaging, flag for removal, or request deep dive investigations from our analyst team into the origins and proponents of specific campaigns. During the three months Logically partnered with the state, our AI ingested millions of individual pieces of content and classified each one. We identified and analyzed 40,000 threats to election integrity and public safety which the team could then review and deploy countermeasures if needed.

6. **Indian 2019 Elections**

During the Indian state of Maharashtra's regional elections in 2019, Logically tackled election related mis and disinformation at scale. In a country in which the number of voters with access to a smartphone—and by extension digital messaging apps—has nearly doubled from 21% in 2014 to 39% in 2019, it's easy to see why such focus was paid to digital campaigning techniques by the main political parties. With the ability for a single person to share a message or story with around 1,280 different individuals in seconds at almost no cost.

For example, from the period of 1st to 30th April 2019, Logically analyzed 944,486 pieces of content and found approximately 27% were fraudulent.

7. **UK elections**

During 2021, Logically provided election monitoring support ahead of and during local government elections in England and Wales, and the national elections of the Scottish Parliament, Welsh Assembly and Northern Ireland Assembly. There were several areas of focus for the client, including identifying any coordinated inauthentic activity foreign state actors, content around public safety, identification of trends and narratives involving the undermining of the democratic process, mis and disinformation targeting vulnerable and minority communities, mis and disinformation related to COVID and the election. The scope of the project ranged from spotting identifying anywhere between 1000 to almost one million pieces of harmful content. Logically provided early warnings on a number of sophisticated efforts to seed a vote rigging narrative. This enabled the local governments to concentrate their strategy and disrupt the narratives before they took hold. Furthermore, coordinated inauthentic activity was also detected and provided to platforms for review and takedowns.

Section 2 – MDM Solution Overview

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] involved in attacking the integrity of an election,proposing violence, spreading mis and disinformation against people and places, or causing doubt about the efficacy of the vote – have moved off the well-known platforms such as Twitter and Facebook and instead exist across a myriad of other social media sites. As a result of our constant monitoring, we continually add new fringe platforms of relevance. These platforms are automatically included as part of our monitoring capabilities and will be utilized in support of SOS.

[redacted]

[redacted]

[redacted] We recognize the need to identify narratives before they reach virality. Our tech provides our users with a steady stream of emerging narratives. By offering this emerging narrative output, we return the information advantage so our clients can make decisions early. Identifying trends in real-time as they start to surface and getting ahead of them can not only save costly extensive endeavors after the fact before they escalate, but doing so can prevent these narratives from continuing to gain traction and ultimately prevent real-world harm.

A. Our platform is the result of more than four years of AI and Natural Language Processing (NLP), Research and Development and continues to be used to understand the evolving misinformation landscape and mitigate its harmful effects at scale.

For example, our automated fact checking system not only classifies false intelligence but tells you why it is inaccurate

B. Our Intelligence platform has been developed to monitor, analyze, and counter misinformation in multiple languages.

C. Patient Zero or Origin Account Identification: Our tech automatically

identifies the origination account for a narrative. This has been proven to be a decisive feature in our previous electoral work. Why? With the knowledge of who originated a narrative comes the ability to more effectively counter false narratives.

We Are NEVER Playing Catch-Up

We have already started collecting data on the 2022 midterm elections and we have developed a baseline for the Oregon election information environment.

- We are collecting data NOW, and have been doing so for quite some time on the 2022 election environment. Our broader collection will enable Oregon to observe national trends and be prepared for MDM threats as they interact with the Oregon electoral environment.

[redacted]

Our platform is able to identify potentially harmful content not just from social media sites but also from obscure corners of the internet such as the comments sections of blogs and news articles.

- Logically stores and organizes collected data in an easily accessible and secure format in the cloud using Google Cloud or a custom-built system. Data can be searched by keyword, date, file type/format, and the place of origin. Our platform has the ability to transfer intelligence to law enforcement partners as needed. We keep a record of the social media activity we ingest and provide detailed reports that, in the past, have been used in judicial investigations.

- Civil liberties and privacy. We recognize the incredibly powerful capabilities we possess. All data we collect and how it is managed and protected will be compliant with Oregon and federal law.

[redacted]

Official campaign and government accounts are subject to being spoofed. For example, nefarious actors may replace a ".gov" with a ".com" or create a Twitter account so it appears to be the official account of a person or an organization, but, in reality, is fictitious. This has caused confusion among the voting public and undermined the efficacy of the voting process. We offer unlimited monitoring of SoS/OED/CC and campaign accounts, as well as an alerting system so officials or candidates can be made aware should such activity occur.

2. Notification Capabilities

Logically provides a notification system, a customized dashboard, sync meetings, and written updates. We customize the reporting channels to meet client needs.

Additionally, our work is backed by our analyst cadre worldwide depending on the need (for example, during increasing levels of threat to persons, a crisis situation, or during the peak period of election activity), which would allow for full coverage of SoS/OED/CC operations on a 24/7 basis.

Logically pushes alerts and enables decision-makers to proactively understand potential threats and harmful narratives before they result in real-world consequences.

a. **Physical Threats:** Protect people and physical assets (Our platform allows us to adapt and provide SoS/OED/CC officials risk protection in this realm as needed). Logically offers threat monitoring for every member of the combined Oregon team (candidates, state and county workers, and facilities).

b. **Undermining the Electoral System:** Maintain election integrity by mitigating the impact of harmful narratives on electoral procedures, outcomes, and processes.

3. Reporting Capabilities

Logically exists to detect, alert, and respond to social media and digital attack surfaces that pose risks to a government's electoral system. We recognize that a critical step to this process is automated reporting capabilities. Our platform includes customized reporting templates and an export (CSV or PDF) function that includes any page or piece of content. Specifically, our reporting capabilities include:

a. Customized reports to SoS/OED/CC staff.

b. Regular reporting (cadence to be determined with the SoS/OED/CC) on trending MDM topics and threats.

c. Reports identifying what counter-narratives are effectively reaching targeted audiences.

Logically's reporting functionality allows you to visualize narratives and threats within a time frame that best suits your needs. The results generated are automatically added to either a PDF or PPT, making presenting your reports that much easier.

4. Communication Capabilities

We understand SoS's need for managing authoritative public information that refutes MDM narratives. Logically is an accredited member of the International Fact Checking Netw mplete our ability to determine if a piece of content is reliable we offer fact checking as a service. Requests for fact checking can be sent in for free from the voting public on our Logically mobile app. For our paying clients a faster and higher level of fact checking is part of our services. To make determinations if a claim of social media is accurate, we use a combination of AI and humans in the loop.

Logically boasts the world's largest team of dedicated fact-checkers, supported by in-house journalists, innovative technology and efficient, streamlined processes designed to safeguard the integrity of our fact-checks while maximizing their efficiency. While we aspire to a fully automated fact-checking olution, we have developed a hybridized process which supports the development of our fact-checking algorithms, enables the incremental adoption of our automated fact-checking technology as it matures, and enables efficient and high-quality fact-checking in the meantime.

- **Incoming Claim**
  - Users can submit claims for fact-checking that they encounter within the Logically app, or from third party publishers by sharing the article with Logically or pasting the URL into the app. Once we have the article, our claim detection technology gets to work extracting the factual claims within, enabling the user to select the one they'd like verified and submit it to our fact-checkers. Users can also enter raw text or past a message/post from another platform.

Claims then appear on the bespoke dashboard developed to help our team progress claims through our process efficiently, maximizing our chances of preventing false claims from spreading.

- **Automated Factcheck.**
  Incoming claims are first checked against our single source of truth databases through a vectorized analysis of the incoming claim against related claims. This represents an initial processing stage of a larger scalable automated fact-checking solution which will become more efficient as our universe of known and inferred 'facts' is expanded through human fact-checking and sourcing from single sources of truth databases such as Government datasets.

  Additionally, users are able to determine if images are manipulated via the Logically app. The analysis of the image is returned to the user within seconds with color coded highlights on all areas the models believe likely to be manipulated. Users can forward the same image for fact-checking if they would like the content of the image itself verified.

- **Random Sample Verification.**
  Logically conducts random verifications of claims fact-checking through our automation capabilities to ensure that any errors are detected and used to develop the algorithms which conduct the fact-check.

- **Human Fact-check.**
  All claims sent to our human fact-checking team are subject to the following process.

  1. **Selection and Prioritization.**
     We classify all incoming claims according to our taxonomy of claims types. Thi helps us quickly identify unverifiable claims which don't require human attention, and prioritize claims according to their relevance, virality and estimated verification time.

  2. **Assignment.**
     A moderator or supervisor will assign an incoming claim to one of the teams based on the complexity of the claim and the level of research required for verification.

  3. **Research and Conclusion.**
     Our fact-checkers are trained to follow carefully constructed processes according to the type of claim they're verifying, which can be either

statistical or text based. We provide full justification for our judgment, and links to relevant primary sources used to conduct the fact check.

4. **Moderation**

All completed fact-checks must be signed off by a moderator before publication to ensure that the judgment is correct and the justification convincing and substantiated. Fact-checkers can escalate difficult claims to moderators and supervisors as needed, should they be unable to verify its accuracy.

5. Built-in Countermeasures

Our countermeasures program enables the opportunity for unlimited takedown attempts. We provide you with a continually updated list of the accounts which are inauthentic, factually inaccurate, toxic, or posted with the intent to cause harm. Additionally, Logically is already a trusted entity within the social media community and has a preferred status that enables us to support our client's needs at a moment's notice.

Step 1: Item is flagged as MDM through our AI and machine learning models

Step 2: The user creates a countermeasure

Step 3: A dedicated client success manager will follow up with the SoS and either the social media platform or relevant authority.

6. Investigations and Analysis

In addition to our countermeasures feature, we also include "Requests for Investigations" in our platform. Using this tool, clients are able to flag a particular piece of content or account for our analyst team to investigate further.

Step 1: Identify a troubling piece of content

Step 2: Request an investigation from our world-class professionals

Step 3: The scope of the investigation will be determined by the client success manager and the relevant SoS representative. We return a report within 24 hours for a priority lead.

Key differentiators that make Logically uniquely positioned to provide digital risk management services to the SOS

The vast majority of our competitors do not have the ability to process and conduct cross platform analysis in a single dashboard. For example, understanding the interaction between multiple social networks such as 4chan, Reddit, Twitter and Facebook is crucial to understanding the dynamics of misinformation and disinformation. We isolate the origination of claims and identify crossover points – when claims spread from niche groups and networks to broader communities and identify crossover agents – individuals/accounts responsible for pollinating.

Patient Zero

Logically enables our users to quickly (within seconds) identify "patient zero" or the originator of a social media post. The platform enables users to see how a narrative spreads from patient zero across multiple social media platforms. The power of this feature is essential for counter messaging and threat identification.

In cases where imminent harm or outsized harm may occur, our team of OSINT professionals have unmasked many threat actors who did not want to be found.

For example, Logically has identified dozens of anonymous QAnon influencers, two of which were exposed publicly on the basis of their high profiles and importance to the movement: Jason Gelinas (QAPPANON) and Robert Cornero Jr. (Neon Revolt).

Logically was responsible for the successful identification of Jason Gelinas, which was independently corroborated by multiple major media outlets including Bloomberg and the Financial Times. Gelinas was a cyber security expert for a major wall street bank, and had successfully operated a vitally important piece of online QAnon infrastructure in complete anonymity for over two years. Despite extremely sophisticated operational security on Gelinas' part, our team was able to identify him using a mixture of domain analysis, granular OSINT research and Logically's people investigations technology. Gelinas' site was taken down immediately following Logically's exposé.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 3 – Response to Non-Functional Requirements

Availability & Scalability

Access to Logically Intelligence includes unlimited users. Our pricing structure does not have a limit on the number of users. We will create accounts for as many users as the SOS determines is prudent.

Logically provides a team of dedicated analysts to support SoS/OED/CC operations. Additionally, SoS/OED/CC is backed by our analyst cadre worldwide as needed (for example, during increasing levels of threat to persons, a crisis situation, or during the peak period of election activity), which would allow for full coverage of SoS/OED/CC operations on a 24/7 basis.

Security

One of the benefits of having dozens of engineers on staff is that we constantly try to break our own security systems. We continually update our cyber security protocols and monitor every online interaction for attempted breaches. We carry out the basics such as two part authentication up to running the most sophisticated operations to protect our content and software.

Logically follows industry standard security governance procedures and is in the process of complying to ISO/IEC 27001, we use a combination of high levels of encryption, trained staff, and information security policies and technical and Ethical safeguards to protect our customers' data.

Logically uses a combination of internal and third party teams to detect vulnerabilities in our services, as well as continuous Pen Tests (minimum once per year) and offers bug bounties for non critical parts of our service. Logically uses Google Cloud infrastructure which performs regular testing for vulnerabilities.

Our services are backed by robust technical and organizational safeguards, and dedicated security and privacy teams. Our data is encrypted both at rest and during transmission, and we have measures to prevent DDoS attacks by throttling based on IPs. Data access is restricted to only key personnel working on specific projects. Our servers are hosted in Virtual Private Clouds inside Google Cloud Provider, which provides an additional layer of security to the protections already provided by Google.

Auditability & Integrity

Logically ingests data and maintains it in the Google Cloud environment. All aspects of interface with the software and data is recoverable and can be provided to the client on request. Furthermore, Logically's audit team conducts quality assurance checks to ensure the software is being used for the express purpose for which it is intended.

Section 4 – Professional & Support Services

Meet Our Team

Tanveer I. Kathawalla, Logically General Manager, Vice President

Tanveer I. Kathawalla is a national security venture capitalist and executive who has led, scaled, advised, and invested in over ten companies focused on the national security

space. He is currently a fellow at the National Security Institute at George Mason Law School, a member of Leadership Now (a group of business leaders focused on democracy reform), and a Venture Partner at NextGen Venture Partners, an early-stage investment firm. He was the COO/CFO and part of the founding team at Analytical Space, a venture-backed national security satellite company that launched the first commercial cube satellite equipped with a laser. Additionally, he was named a Global Shaper at the World Economic Forum in 2014 and an Aspen Ideas Scholar in 2017. Tanveer earned his bachelor's degrees from the George Washington University in political science and economics, is a graduate of the Sorensen Institute of Political Leadership, and is an MBA candidate at the Darden School of Business at the University of Virginia.

Brian Murphy, Logically Vice President

Brian Murphy is an expert on mis/disinformation and social media and its relationship to radicalism. As an adjunct professor, he has designed and taught curriculum for Georgetown University's Security Studies Program on extremism and the intelligence process in the US. Prior to joining Logically, he was the Acting Under Secretary for the Office of Intelligence and Analysis. In that role, he was responsible for the conduct of key intelligence functions supporting the Department of Homeland Security, including all intelligence activities for the Department pertaining to elections and threats.

Before joining DHS, Murphy was responsible for several national security programs at the Federal Bureau of Investigation during which the threat from hostile nations was a centerpiece. Murphy created, ran, and organized the FBI's CVE programming. Murphy was appointed to the Senior Executive Service in 2016. He is also a veteran of the U.S. Marine Corps. He earned a Bachelor of Arts in Government from the College of William & Mary, a Master's degree in Islamic studies from Columbia University, and is finishing his doctorate at Georgetown University. His doctorate is on disinformation and democracy. Murphy's most recent publication is "Decaying National Security: Understanding the Implications of Imagined Tribalism and its Connection to the Decay of Nationalism in a Radically Changed Information Context" - RUSI Journal | Royal United Services Institute. Among his awards were the 2020 award for excellence by DHS • 2003 and 2007 recipient of the Attorney General's Award for Excellence in • 2006 and 2006 National Security Investigations and nominated for the FBI Director's Award • 2005 NYC Counterterrorism Investigator of the Year • 2001 and 2005 received the United States Attorney's Award for Excellence in National

Security Investigations.

Kelsey Ritchie Frierson, Client Success Manager

Kelsey Ritchie Frierson is a subject matter expert in identifying and countering disinformation, particularly related to elections. She has a breadth of practical experience having worked with a variety of government agencies on disinformation investigations and analyses. Previously, she worked for Deloitte's federal consulting practice, where she managed the creation of the Countering Malign Influence Fusion Center and co-led the Countering Mis/Disinformation Community of Interest. During the 2020 US general elections, she led a team of analysts on a project for the Cybersecurity and Infrastructure Security Agency (CISA) tasked with identifying mis- and disinformation related to mail in voting, election fraud, and political violence. She conducted in-depth analysis on the potential for political violence resulting from the online information environment. She regularly briefed state and federal level elected officials on election-related mis-, dis-, and malinformation. Her in-depth analysis has covered domestic extremism, COVID-19, QAnon, hostile nation information warfare, and political violence. She received her Master's in Global Policy Studies with an emphasis in national security from the LBJ School at the University of Texas, where she wrote her Masters thesis on the radicalization of foreign fighters, particularly in Western countries. She received her undergraduate degrees in Political Science and Journalism from Texas Christian University.

Pamela De La Rosa, Senior OSINT Analyst

Pamela De La Rosa is a recent graduate with a Masters in international cybersecurity policy with a focus on disinformation. Pamela is an expert on researching and analyzing disinformation campaigns and narratives in the United States, Latin America, and Europe and the Middle East. Prior to joining Logically, Pamela was an Open-Source Intelligence (OSINT) Consultant at Meta via Pinkerton where she identified and reported on dangerous organizations and peoples, disinformation, and extremism on Meta’s family of apps and services.

Dr. Anil Bandhakavi, Head of Data Science

Anil heads the data science and machine learning operations with more than ten years of experience in the field of Artificial intelligence, including a Ph.D. in NLP. He has technical leadership experience in developing effective AI solutions that enable the tools and products. He believes strongly in extended (artificial + human) intelligence to create impactful and interpretable solutions to societal problems.

Publications:

- *Anil Bandhakavi*, Tanmoy Chakraborthy Would your tweet invoke hate on the fly? forecasting hate intensity of reply threads on twitter. Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining (SIG KDD 2021)
- *Anil Bandhakavi*, Nirmalie Wiratunga, Stewart Massie, Rushi Luhar Opinion Context Extraction for Aspect Sentiment Analysis. Proceedings of the Twelfth International AAAI Conference on Web and Social Media (ICWSM 2018)
- *Anil Bandhakavi*, Nirmalie Wiratunga, Stewart Massie, Deepak.P *Lexicon Generation for Emotion Detection from Text*. In IEEE Intelligent Systems, 2017
- *Anil Bandhakavi*, Jeremie Clos, Nirmalie Wiratunga *Predicting Emotional Reaction in Social Networks*. In proceedings of ECIR, 2017
- *Anil Bandhakavi*, Nirmalie Wiratunga, Stewart Massie, Deepak.P *Emotion-corpus based Sentiment Lexicons for Twitter Sentiment Analysis*. In proceedings of BCS SGAI 2016, Cambridge, UK
- *Anil Bandhakavi*, Nirmalie Wiratunga, Stewart Massie, Deepak.P *Lexicon based Feature Extraction for Emotion Text Classification*. In Elsevier Pattern Recognition Letters on Data Mining, 2016
- *Anil Bandhakavi*, Nirmalie Wiratunga, Deepak.P, Stewart Massie. *Generating Word-Emotion Lexicon from #Emotional Tweets*. In proceedings of *SEM 2014, Ireland

Training and Deployment

Easy to use dashboard and reporting targeted at both technical and executive users; Training provided.

For frequent users: We offer four training blocks for the core users who will be using our platform on a routine basis. Logically Intelligence's (LI) intuitive design allows analysts to make the most of the platform without specialist training. There is thorough documentation and expert technical support on hand to aid LI users.

For executive users: We modify our training block to meet their busy schedules. All users will have access to a built-in reports function which in a keystroke provides a customized report.

Logically's 24/7 operation and analysts work to find the original source, and the matrixed networks connected to the original source. We pride ourselves on setting the standard for proactively identifying threats for our clients. As a result, our clients can diffuse these efforts immediately upon identification, and begin mitigating the

aftermath and damage – preventing further escalation and therefore, protecting the integrity of their efforts and democratic institutions.