Maximize Safety and Minimize Risk for Large-Scale Events and High-Profile Clients

Advance Warning: Using OSINT to Improve Security for Events, Venues, and VIPs

BABELSTREET

Introduction

At a 2024 campaign rally in Pennsylvania, a young gunman wielding a semiautomatic rifle fired at least eight times before Secret Service agents killed him.[1] The shooter hit former president Donald Trump, wounding his ear. He also murdered a 50-year-old volunteer firefighter.[2] Later, law enforcement searching the gunman's van found explosives and a detonator.[3]

This tragedy illustrates why a comprehensive security plan for high-profile events is critical for protecting VIPs, guests, and the venue itself. This e-book will discuss how open-source intelligence (OSINT) can help in this effort.

The event security landscape

Securing high-profile events from terrorism, mass shootings, or other acts of violence is a challenging and increasingly sophisticated process. Host organizations need comprehensive security strategies for every type of high-profile event — from campaign rallies to Wimbledon, from G20 Summits to pop concerts.

Law enforcement, corporate security teams, private security teams, and security consultants — often working in tandem — must employ every available tool to defend these events, implementing measures to protect guests, venues, and of course, "stars" — the corporate executives, political leaders, athletes, celebrities, and other VIPs people gather to see. They must provide this protection at three points on the timeline: before, during, and after the event.

Security professionals see a growing need for this type of comprehensive protection. Trump's would-be assassin wasn't the first shooter or terrorist to cause mayhem at a high-profile event.

In April 2013, brothers Dzhokhar and Tamerlan Tsarnaev planted two homemade bombs hidden in backpacks near the finish line of the 117th annual Boston Marathon. The bombing, motivated by United States involvement in Iraq and Afghanistan, killed three people. Hundreds more were injured, including 17 people who lost limbs.[4] Four years later, an extremist suicide bomber murdered 22 people and injured more than 1,000 others in England's Manchester Arena immediately following an Ariana Grande concert.[5] The deadliest mass shooting in United States history took place in 2017 in Las Vegas, when a gunman opened fire on the Route 91 Harvest music festival. Sixty people were murdered and more than 850 injured.

Law enforcement and security teams have traditionally deployed physical measures to counter threats of physical harm. These include:

- Controlling event access with perimeter fencing and metal detectors
- Stationing security personnel at strategic points throughout the venue, most notably near VIPs
- Working K-9 dogs trained to find the scent of explosives
- Implementing clear-bag policies
- Deploying surveillance cameras to spot threats and deter bad actors
- Implementing emergency response protocols for medical situations, mass shootings, and other disasters
- Establishing crowd management processes to ensure the safe movement of attendees into, out of, and through the venue
- Positioning counter-snipers at outdoor events

But as the attacks above illustrate, it's not enough.

For optimal security, law enforcement and security professionals need the situational awareness and threat awareness that OSINT provides. OSINT is intelligence gleaned from the processing and analysis of publicly available and commercially available information (PAI/CAI). Through social media monitoring, semantic understanding, name matching, and other capabilities, OSINT technologies can help law enforcement and security professionals better identify and prevent threats to high-profile events.

Using OSINT to protect guests and venues

Before the event

"You kill innocent women and children by doing us airstrikes..now taste the Islamic state vengeance. In the next few days you will see attacks from the Islamic State in the usa."[6]

This post was written on June 12, 2016, by a social media user living on Florida's east coast. That night, he murdered 49 people and wounded 53 more at the Pulse nightclub in Orlando.[7]

By identifying potential threats in near-real time and alerting law enforcement to these threats, the right OSINT solution can help prevent tragedy. Law enforcement agencies and security firms can use OSINT solutions to monitor social media, online forums, news outlets, and other sites for indications of planned attacks or disruptive behavior targeting specific events, venues, or populations.

What could an OSINT solution have told law enforcement and security teams about the Pulse shooter?

- He wrote a threatening post
- The post warned of near-term violence
- It expressed support for the Islamic State (a terrorist group better known in the United States as ISIS or ISIL)
- The violence planned would align with the ISIS worldview
- He lived in Florida

With this information in hand, law enforcement may have determined that this social media user needed to be investigated quickly. Especially if they had learned that the FBI had twice investigated the user for potential terrorist ties.[8]

The Pulse shooter's social media post is not an aberration. Broadly speaking, mass shooters and some terrorists tend to announce their plans online.[9] For example, before murdering ten Black people at a Tops Friendly supermarket in Buffalo, N.Y, the white supremacist terrorist declared his plans in his Discord journal.[10] Before killing 23 people at a Texas Walmart in 2019, the murderer used social media to discuss his hatred for Hispanic people and announce his intentions.[11]

Most of us feel upset when we see social media posts threatening violence or terrorism. But these posts can actually bolster security efforts by providing law enforcement and security professionals with the intelligence needed to stop these acts before they cost lives.

Often, threatening posts are blunt — unmistakable in their intent OSINT solutions can detect them. But the social media monitoring capabilities of the best OSINT platforms can also help security professionals find more subtle indications of the potential for violence. How? Online, a forger may advertise for sale fake credentials, such as those that give legitimate staff back-stage access. Certainly, those interested in buying these credentials may be over-zealous fans intent on meeting their musical idols. They may also be criminals who'd like the notoriety of murdering an entertainer, or terrorists seeking the ability to place bombs near building supports for maximum destruction.

In addition to social media threat monitoring, OSINT solutions can help with physical security assessments prior to an event. Security teams can look for information that's already publicly available for specific locations, such as floor plans, vehicle access, loading docks, etc. If this type of information could be used to gain access to a venue by someone planning an attack, then security teams should factor it into their response plans.

During the event

Social media monitoring for guest and venue protection doesn't stop once the doors open. Rather, examining social media during high-profile happenings can help with crowd monitoring — providing insights into the mood of guests, who often post during the game, meeting, or concert. This information can help security teams anticipate crowd management challenges and adjust security and response plans accordingly.

In addition, attendees may spot and post about signs of trouble even before security professionals become aware of them. At a major event in 2023, one patron Tweeted, *"If you are in the [Major City] arena please be careful! This guy is making claims of a mass shooting!"*[12] Social media monitoring can alert law enforcement and security to posts like these.

While mass casualties are every venue's worst fear, OSINT social media monitoring capabilities can also help spot and stop lesser crimes. It interprets coded language to aid security professionals in handling crimes taking place at the event.

Consider this example: *Hanging out in Seat 23C, waiting on Aunt Hazel. #HighProfile Sporting Event #MajorArena*. "Aunt Hazel" is code for heroin.[13] This patron is looking to buy, and telling dealers where he can be found. Alternately, security professionals may uncover a post reading something like, *Am really enjoying my view from seat 15B.* ❄❄❄❄❄❄❄❄❄❄❄❄ Snowflake emojis are code for cocaine.[14] The poster is letting people know where to buy the drug. High-profile events also sometimes act as vectors for human trafficking. Posts such as, *Daddy, your angel is ready for anything. Visit me in Section 3, Seat 4* may indicate the use of trafficked women being offered for sex.[15]

Social media monitoring for guest and venue protection doesn't stop once the doors open. Rather, examining social media during high-profile happenings can help with crowd monitoring — providing insights into the mood of guests, who often post during the game, meeting, or concert.

After the event

Perhaps fearing security at the venue itself, terrorists and others may think the parking structure is the perfect spot to place a bomb, or to stage a mass shooting. An argument brewing among opposing fans at a soccer match may spill over into violence outside the arena. A drug dealer may be advertising for people to meet him at a given parking spot if they want a hit for the road. Combing OSINT with local knowledge of crime patterns can help law enforcement and security professionals spot spill over violence and stop these crimes.

If crimes do occur, OSINT can help bolster prosecution against perpetrators by uncovering video footage from the attack, social media posts from witnesses or participants, and other incriminating evidence. Even if these posts are quickly deleted from a platform, an OSINT solution may have preserved them in its archive.

Protecting VIPs

VIPs benefit from the same security efforts that guests do: a bomb placed in a concert venue can just as easily kill the singer as the guest in seat 16B. But VIPs' visibility and status leave them facing specific security challenges. Smart use of OSINT, in addition to traditional security measures, in addition to traditional security measures such as bodyguards, can do much to mitigate these threats.

VIPs may face threats traveling to and from a venue. Some of these are general risks that anyone might face: the uncertainties inherent in traveling to a politically unstable country, for example, or the risk associated with traveling to a geographic region prone to hurricanes, tornadoes, or other natural disasters. Being stranded by a hurricane is a problem for anyone. But these situations have broader ramifications for VIPs. Can a company in the middle of a merger or acquisition afford to have its C-suite stuck in a Florida hotel room for a week with only limited communications?

Before, during, and after the event, VIPs also face more targeted threats. The head of an oil company may face protests from environmentalists. A splinter group associated with one political party may loudly and violently decry what it perceives as the evils wrought by the leader of another political party. These threats can continue as VIPs make their way home. After the event, VIPs and their organizations also face the threat of reputation attacks and deepfakes.

What are these attacks?

In an attempt to harm an executive or smear corporate reputations, digital campaigns may be launched against a VIP or company. Often, these campaigns contain false, inflammatory, or defamatory information. Deepfakes — or AI-generated audio or video — may be used to discredit VIPs. Alternatively, the creator may manipulate actual footage to make it seem as if leaders have said or done something they haven't. Deepfakes of Rishi Sunak, then prime minister of the United Kingdom, appeared on Facebook, TikTok, X, and Instagram in advance of the 2024 prime ministerial election.[16] These deepfakes claimed, among other things, that the government of the United Kingdom planned to invest in a stock market app created by Elon Musk.[17] Sunak lost the election. (The effect of the deepfakes on voting patterns has not been determined.)

In identifying threats to VIPs, OSINT technologies can help law enforcement and security professionals take the steps needed to mitigate them.

Finding the right OSINT solution

A number of OSINT solutions are now on the market. How do you find the one that best suits your needs? For the protection of venues, guests, and VIPs at high-profile events, security leaders should look for solutions that:

- Scan a huge volume and variety of PAI/CAI
- Enable better searches
- Provide AI-powered semantic understanding of social media posts and other online content to look beyond the words used to the intent of those words

Sources scanned should include established and emerging social media sites: not just Facebook, LinkedIn, and Instagram, but platforms such as Truth Social, Kick, and Bluesky; not just mainstream message boards like Reddit, but niche boards such as 4Chan and 8kun. They should examine sites that host varying types of media, including video sites such as TikTok, YouTube, Vimeo, and streaming communities. Along with reputable news sources, your solution should search blogs hosted on WordPress and similar sites.

Smarter searching ensures you find the information you need from the sources examined. Two capabilities to look for are persistent search and translation. Persistent search is a technology that keeps a search operation running regardless of whether someone is actively using it, appending newly found information to existing search terms.

All the OSINT in the world does law enforcement and security professionals no good if they can't understand the language in which it is written. Therefore, your OSINT solution must be capable of finding information published in a broad variety of languages, then translating it into your language of choice.

As mentioned above, threats aren't always easy to spot. Certainly, OSINT solutions maintain lists of threat words to search. (Words such as "annihilate," "carnage," and "bleed out" tend not to appear in everyday Facebook updates.) But similar words and phrases can indicate very different intents. That's why semantic understanding is so important. A singer posting, *I tore up Very Big Arena last night. Shout out to the audience for making it happen!* 😊😊😊 is very different from a disturbed individual posting *I'm going to shoot up Very Big Arena tonight. I can't wait to hear the audience shout out* 🔫.

Semantic understanding can also help organizations understand new representations of words. It can search for emojis meant to evoke violence: skulls, bombs, swords, and others. It can detect codes and symbols used to denote drug sales. Finally, it can help detect coded hate speech — a significant benefit to venues hosting events geared toward populations that are often subjected to bigotry.

How Babel Street can help

The Babel Street AI-powered ecosystem delivers advanced data and analytics solutions that transform diverse data sources into actionable insights. Babel Street Insights provides persistent searches of thousands of sources of PAI and CAI. To provide security professionals and law enforcement with the insight needed to secure venues and events, our technology scours data sources published in more than 200 languages and translates results into the user's language of choice. Information sources include more than a billion top-level domains, commercially available sources, and real-world interactions generated on chats, social media posts, online comments, and message boards.

Insights further enhances security through searches of the deep and dark web — or websites that are inaccessible by standard search engines. Because the nature of the tools used to access the dark web ensure anonymity, it is a hotbed of illegal activity. Dark web search capabilities enable investigators to scan posts and other information they wouldn't otherwise be able to see.

Situational awareness and threat awareness are vital components of any comprehensive security program. Babel Street can help law enforcement and security professionals better analyze PAI, CAI, and hidden web data for insights into the type of information that indicates potential criminal activity aimed at venues, guests, or VIPs. It helps security professionals better identify entities and their relationships with each other. In doing so, Babel Street technology can help law enforcement and security professionals better secure high-profile events.

How does it work?

Law enforcement and security teams use Babel Street technology to search for specific "red flag" keywords that may indicate a threat. In the case of direct, violent intent, Babel Street Insights can flag the post, note its author, then search the author's other online identities/accounts and activities. Babel Street can even link the author's screen name to a real-world person and provide his or her contact information.

Our technology further pinpoints groups whose activities may interest law enforcement (i.e., splinter group associated with a political party, protesters, terrorist groups). With Babel Street, security analysts can map the relationship of individual social media accounts to the social media accounts belonging to that group; identify the most influential accounts; then closely monitor the posts from those accounts.

Security teams can also use Babel Street to monitor geopolitical and geographical situations worldwide, a capability helpful for VIP protection. Searches for kidnapping trends will quickly enable analysts to learn that Nigeria has a kidnapping crisis, spurred by poverty, political unrest, and religious extremism. Understanding this, security teams may discourage an executive from attending a conference in that country. Searches can also unveil political instabilities, natural disasters, and areas prone to riots or demonstrations. Similar capabilities help security teams spot and stop reputational attacks and deepfakes.

These capabilities are not theoretical. Before the 2023 Formula 1 Grand Prix in Las Vegas, a private security firm worked with Babel Street to uncover and mitigate risks to the venue, guests, and drivers. Babel Street was able to help this firm identify a group of individuals, based in Las Vegas, who planned to disrupt the event. Babel Street accomplished this by uncovering patterns and connections among these individuals that were hidden within massive data sets. That same year, a Babel Street client spotted a post in which the writer threatened a mass shooting — even naming the individuals he planned to target. Using pivotal information generated by Babel Street Insights, law enforcement officials tracked down the would-be murderer. The man, who had access to firearms and hand grenades, was arrested before he could put his plan into action. Similar Insights capabilities helped European law enforcement spot and monitor a man whose posts indicated he planned to shoot up a family planning center.

Securing high-profile events from terrorism or other acts of violence is a challenging process. While physical protection measures remain important, technological offerings such as innovative OSINT platforms provide law enforcement and security professionals with an edge: the opportunity to uncover violent intent before the unthinkable happens, and uncover supporting evidence to build a case against the perpetrators.

Endnotes

1. Levenson, Michael, "What We Know About the Assassination Attempt Against Trump," The New York Times, July 2024, https://www.nytimes.com/2024/07/14/us/politics/shooting-trump-rally.html
2. Ibid
3. Eberhart, Chris, "Police comb through Thomas Matthew Crooks' van that hid explosives, video shows," Fox News, July 2024, https://www.foxnews.com/us/police-comb-through-thomas-matthew-crooks-van-hid-explosives-video-shows
4. Wikipedia, "Boston Marathon bombing," accessed July 2024, https://en.wikipedia.org/wiki/Boston_Marathon_bombing#:~:text=During%20questioning%2C%20Dzhokhar%20said%20that,was%20following%20his%20brother's%20lead
5. Wikipedia, "Manchester Arena bombing," accessed July 2024, https://en.wikipedia.org/wiki/Manchester_Arena_bombing
6. ABC News, "Orlando Shooter on Facebook: Now 'Taste' ISIS 'Vengeance,' June 2016, https://abcnews.go.com/US/orlando-shooter-facebook-now-taste-isis-vengeance/story?id=39875518
7. Wikipedia, "Pulse nightclub shooting," accessed July 2024, https://en.wikipedia.org/wiki/Pulse_nightclub_shooting
8. Wikipedia, "Pulse nightclub shooting," accessed July 2024, https://en.wikipedia.org/wiki/Pulse_nightclub_shooting
9. Peterson, J., Densley, J., Spaulding, J., & Higgins, S., "How Mass Public Shooters Use Social Media: Exploring Themes and Future Direction," Social Media + Society, accessed July 2023, https://doi.org/10.1177/20563051231155101
10. Suciu, Peter, "Social Media Increasingly Linked to Mass Shootings," Forbes.com, May 2022, https://www.forbes.com/sites/petersuciu/2022/05/25/social-media-increasingly-linked-with-mass-shootings/?sh=45b045aa3c73
11. Lee, Morgan and Weber, Paul J., "The Texas Shooter in a Racist Walmart Attack is Going to Prison: Here's What You Need to Know About the Case," Associated Press, July 2023, https://apnews.com/article/el-paso-walmart-texas-crusius-bf7d25f3567959ee8b121deabcf1d9a1
12. Babel Street Insights, 2023
13. DEA Intelligence Report, "Slang Terms and Code Words: A Reference for Law Enforcement Personnel," July 2018, https://www.dea.gov/sites/default/files/2018-07/DIR-022-18.pdf
14. Babel Street internal research
15. Babel Street internal research
16. Criddle, Cristina, "Political deepfakes are the most popular way to misuse AI," Financial Times via Ars Technica, June 2024, https://arstechnica.com/ai/2024/06/political-deepfakes-are-the-most-popular-way-to-misuse-ai/
17. WION, "Deceptive Facebook ads with de fake UK PM Rishi Sunak," accessed July 2024, https://www.youtube.com/watch?v=dX8fxhqZo4s&ab_channel=WION

Babel Street is the trusted technology partner for the world's most advanced identity intelligence and risk operations. The Babel Street Insights platform delivers advanced AI and data analytics solutions to close the Risk-Confidence Gap.

Babel Street provides unmatched, analysis-ready data regardless of language, proactive risk identification, 360-degree insights, high-speed automation, and seamless integration into existing systems. We empower government and commercial organizations to transform high-stakes identity and risk operations into a strategic advantage.

Learn more at babelstreet.com

All names, companies, and incidents portrayed in this document are fictitious. No identification with actual persons (living or deceased), places, companies, and products are intended or should be inferred.

BABELSTREET