IBM - United States

Protecting people and communities with pre-emptive social media threat analytics

When individuals and groups are planning criminal activity, they often signal their intentions online via open source social media. Tactical Institute uses cognitive analytics from IBM to assist in its mission to monitor social channels 24x7, analyze billions of comments and posts, home in on threats, and identify perpetrators before they can act.

> *"Watson Analytics is a force multiplier, a tool that gives each of us the ability to work many times more effectively and productively."*
> —Oliver Oetterer, Chief Operating Officer, Tactical Institute

> *"Giving our analysts the tools to assess a suspect's means and opportunity as well as their motive is potentially a huge win for our team."*
> —Paul San Soucie, Chief Technology Officer, Tactical Institute

Previous

About the client's company

Tactical Institute

Tactical Institute provides real-time, advanced detection and notification of threats issued via open source social media sites, so that clients can take pre-emptive action before the threat is executed. Where other firms sell software products requiring resources and aptitude on the part of the customer, Tactical Institute provides a service in which its analysts—many of whom are combat-wounded veterans—identify threats to clients using proprietary e-tradecraft developed over 25 years in some of the most challenging governmental and private services imaginable.

Business challenge

To help keep its clients safe, Tactical Institute must be able to monitor billions of social media messages and read the subtle nuances that differentiate a harmless tweet from a dangerous threat.

Transformation

IBM® Watson Analytics™ for Social Media helps Tactical Institute analyze social sentiment and evaluate whether a person has the criminal intent, means and opportunity to carry out a particular threat.

Results

The solution acts as a force multiplier, detecting threats that might have been overlooked, minimizing false positives, and helping Tactical Institute identify criminal violence before it occurs.

Preventing acts of violence before they happen

When individuals and groups are planning acts of violence, they often reveal their intentions by posting threats or manifestos on non-private social networks. In many cases, these posts appear less than 72 hours prior to the acts they intend to commit, potentially providing a short window of opportunity for investigators to assess the threat, locate the perpetrators, and prevent the crime from occurring.

However, there is a catch: every day, more than 500 million new messages are posted on Twitter alone. Combined with other social media services, blogs and forums, this adds up to a vast mass of unstructured data. How can you identify the one post that speaks with malevolent intent, against the background noise of hundreds of millions of other online voices? Suddenly that window of opportunity looks more like a ticking clock.

Oliver Oetterer, Chief Operating Officer of Tactical Institute, has an answer: “Social media threat analytics is possible—but it’s difficult and it requires both advanced technology and specialist expertise. We have developed a discipline we call ‘e-tradecraft’, which takes our years of experience in the military and law enforcement and combines it with cognitive analytics. This allows our veteran analysts to sift through huge amounts of data and instantly identify potentially dangerous threats within minutes.”

The e-tradecraft approach has always relied on technology, but until recently, the analytics tools that Tactical Institute was using were not smart enough to reliably evaluate the risk potential of social media content.

Paul San Soucie, Chief Technology Officer, comments: “We were using sentiment analysis, but it lacked subtlety. If someone posted that they would ‘love’ to commit an act of violence, the tool saw the word ‘love’ and assessed the message as positive. Whereas if someone posted ‘Hillary is going to kill Trump in California’, it flagged it as a serious threat. We wanted a more flexible solution that we could configure to assess the context more appropriately.”

Harnessing the power of cognitive analytics

Tactical Institute is one of the first organizations in the world to adopt IBM® Watson Analytics™ for Social Media. Paul San Soucie explains:

“We knew we wanted Watson Analytics because our founder and CEO had used it in other projects and was enthusiastic about its potential. As soon as the social media component came out of beta, we jumped at the chance to build it into our threat analytics process. It currently gives us instant access to data from seven of the most important social sources on the web, providing us with comprehensive coverage of most of the activity that happens on public social networks.”

To help Tactical Institute get up and running and gain maximum value from the solution, Cresco International, an IBM Business Partner, provided social media analytics expertise.

“There’s a great meeting of minds between our organization and Cresco,” says Oliver Oetterer. “They believe in what we’re doing here at Tactical Institute to keep people and communities safe, and we’ve seen them go above and beyond the call of duty to help us. Our use-case for Watson Analytics is a little unusual, and in many ways we’re breaking new ground, so it’s vital to have great support from both IBM and Cresco to keep pushing the boundaries of what’s possible.”

Sanjeev Datta, Practice Director at Cresco International, comments: “Every client is unique and has a unique problem to solve based on their business processes, rules and demands. Our technical team builds with passion, because every day brings a new challenge—and the challenges that Tactical Institute is trying to solve are very close to our hearts. By combining Tactical Institute’s tradecraft with innovative IBM technology and Cresco's experience, we are working together to build stronger and safer communities.”

Together, Tactical Institute and Cresco have built a process that uses Watson Analytics to ingest and analyze the data, assess which tweets, posts and messages suggest a motivation to commit criminal acts, and send leads in the form of URLs to Tactical Institute’s analysts.

Keeping clients and communities safe

Tactical Institute has quickly realized the benefits of adopting IBM Watson Analytics for Social Media, as Oliver Oetterer explains:

“We’re just getting started with the solution, but the advantages are already clear. First, the solution is going to accelerate the way we collect and analyze social media data, which increases our chances of detecting threats and alerting security or law enforcement in time to intervene. Timeliness is everything in our business—if an incident is going to happen today, we can’t take a week to analyze the data.

“Second, the solution gives us better coverage of the social media world, with a wider range of data sources that we can combine with our own research into the dark web and other online sources.

“Finally, it gives us a sharper view of the context of individual messages. Instead of being constrained by a set of standard sentiment dictionaries that don’t understand the nuances of threatening language, we can continually refine our solution to give Watson Analytics the right vocabulary. This will help to eliminate false positives, which can be a wild goose chase for our analysts—and more importantly, it will help ensure that real threats don’t slip through our net.”

Paul San Soucie adds: “We see an even greater role for Watson Analytics in the future. For example, in addition to the sentiment analysis, which helps us understand motivation, we can also use link analysis to detect connections between individuals, their locations, their associates, and so on. This could help us evaluate whether someone actually has the means and the opportunity to carry out a threat.”

“For example, one of our biggest focus areas is threats against schools—we do this as a public service, and we’ve been involved in detecting and pre-empting more than 50 incidents over the past few years. Schools have a definite geographical location, so that factors into the analysis—if someone is threatening violence against a particular school, but they’re posting from hundreds of miles away, that’s less of a red flag than if they’re in the same town. Giving our analysts the tools to assess means and opportunity as well as motive is a huge win for our team.”

Oliver Oetterer concludes: “There’s a military term that many of our veterans like to use: Watson Analytics is a force multiplier, a tool that gives each of us the ability to work many times more effectively and productively. With our old methodology, we might find the top 1,000 threats; with Watson Analytics, we’re thinking it will be more like the top 1,000,000. And in this business, the bigger the haystack, the more needles we are likely to find for our customers.”