RCA for Law Enforcement

February 2012

IBM Enterprise Content Management software

Becoming an Agile Digital Detective

Web-based social networks connect and empower people to find like-minded individuals to quickly fuel their beliefs and causes. While many use this power for positive, constructive use; others use it to spread hate, incite violence and attack the fabric of society on a local, state, national or even global scale.

Providing protective services for our nation in today's world—connected by online social networks—is a daunting task that can keep officers up at night. Controversial legislation can put politicians in the cross hairs; prosecutors and judges can be targeted due to their roles in criminal proceedings, and organizations that are at odds with each other's belief systems can lead to extreme reactions by radical members. Detectives must be enabled to initiate monitoring for threatening messages as a preemptive approach to identifying when rhetoric appears to be escalating into violence.

As a result, today's protectors of the peace must be agile digital detectives that can tap into social networks to uncover and keep ahead of evolving threats against public figures, corporate officers, students, government facilities, citizen organizations and law enforcement themselves.

An effective digital detective investigating a known offender or potential threat must identify the relevant groups and individuals to monitor on social media sites that have the potential to attract radical elements on Facebook communities, Google groups and blogs.

Once surveillance subjects have been identified, be they communities or individuals, the next step is to collect messages from these persons or groups of interest based on keywords. The resulting large volume of data from social media sites must then be distilled and analyzed in order to become meaningful intelligence for law enforcement.

The speed of online social network communication does not afford the luxury of time to manually collect, sort through and analyze this data. The monitoring of the 50 U.S. Governors alone can result in reviewing over 4,000 Twitter messages a day. Addressing the high rate and volume of messages requires automated tools to gain the insight that will prevent an escalating event from evolving into a regretful aftermath.

Another indispensable tool to prevent ominous events is forensic data mining, which allows intelligence to be culled from a large cache of documents that may be obtained via seizure by investigators, SWAT units and officers executing search warrants.

Most of us remember the 4 terabytes of documents seized from Osama Bin Laden's hideout in Abbottabad; each day that went by, the value of the information decreased exponentially as the terrorist network scattered knowing that their locations had been compromised.

The time clock ticks away each day after investigators confiscate notebooks, workstations, USB keys, tablets, smart phones and cameras with terabytes of documents, emails and chat logs in need of digital forensic analysis to find the "needle in the haystack" that could prevent mayhem from materializing.

Forensic data mining can also be of service for "rapid damage assessment" when classified information is leaked onto the Internet. In these circumstances, it becomes paramount to the information owners to quickly assess what they have lost and the extent of risk caused by the unplanned exposure so they may take pre-emptive actions to minimize the harm that may be caused. An example of this would be when over 60 gigabytes of U.S. State Department diplomatic cables were leaked on the web.

Automated threat analysis tools can help address these digital surveillance and data mining challenges, but most tools require linguistics expertise and have traditionally been available only to the most elite law enforcement, public safety and defense agencies. Smaller, local agencies need a way to uncover the digital thumbprint left behind by today's tech-savvy criminal element. They must be able to discover and analyze the clues that are buried deep within diverse content sites.

Uncovering the Digital Thumbprint to Neutralize Threats

ECM Universe's Rapid Content Analytics (RCA) for Law Enforcement brings threat analysis tools – previously available only to elite organizations such as the Department of Homeland Security and other Federal Intelligence Agencies – within the reach of all law enforcement agencies, regardless of size and stature. It enables rapid analysis of on-line content, based on language patterns characteristic of known offenders and credible threats.

RCA for Law Enforcement is a social media surveillance solution providing real-time monitoring of Twitter, Facebook, Google groups, and many other communities where users express themselves freely. The solution employs text analytics to correlate threatening language to surveillance subjects, and alert investigators of warning signs. "Protective Service Surveillance" and "Person of Interest Surveillance" monitoring cases are easily initiated.

RCA for Law Enforcement also provides digital forensic data mining capabilities that enable a roadmap through terabytes of documents that help uncover valuable intelligence.

Once the investigator has identified the online communities that should be monitored (such as Facebook pages, Twitter feeds, blogs, Google groups, forums and newsgroups, wikis and activist and hate group sites), the solution crawls these sites to collect postings and documents.

After the relevant tens of thousands of user posts are collected, the solution's text analytics capabilities, utilizing IBM Content Analytics as the linguistic analysis platform, are put into action to "data mine" for threatening language relevant to an individual or group under surveillance.

The results are readily available for review in a variety of analytic views all emphasizing the actual relevance of threatening language and eliminating the need to sift through thousands of "false positives" or "false leads".

Alert messages are sent to automatically notify investigators when a threatening or suspicious message is posted.

As current events unfold, a city can monitor activist groups who are using social media to organize their efforts on the ground and receive alerts in a matter of minutes from the time of the postings when dangerous radical elements emerge from the crowd.

The results of analysis can be viewed from various graphical visualizations, each of which quickly extract and call out threatening messages.

RCA for Law Enforcement is an agile lightweight solution that can be easily incorporated into existing IT environments in a matter of hours. The solution provides a browser based "analyst" application for data mining and a browser based administration application.

Rapid Content Analytics for Law Enforcement is a game-changer. In a matter of hours, law enforcement analysts can establish new monitoring targets and begin monitoring online social networks for threatening language regarding a specific surveillance target. This allows law enforcement officials to respond quickly to unfolding current events and to dynamically deploy resources to the areas of greatest threat – potentially preventing a riot, hate crime, hostage situation, or other public safety catastrophe. The benefit is safer communities, better use of resources, and optimized force deployment.

For more information, please contact:

Scott Raimist
ECM Universe
+1 703 568 7638
scott@ECMUniverse.com · www.ecmuniverse.com

About EMC Universe

ECM Universe is a certified minority-owned business that implements content analytics, enterprise content management, and eDiscovery solutions for government and commercial organizations. It specializes in IBM technologies. ECM Universe was founded in 2000 and is located in Chantilly, Virginia.

About IBM ECM

IBM's Enterprise Content Management software enables the world's top companies to make better decisions, faster. As a market leader in content, process and compliance software, IBM ECM delivers a broad set of mission-critical solutions that help solve today's most difficult business challenges: managing unstructured content, optimizing business processes and helping satisfy complex compliance requirements through an integrated information infrastructure. More than 13,000 global companies, organizations and governments rely on IBM ECM to improve performance and remain competitive through innovation.

IBM Corporation
3565 Harbor Boulevard
Costa Mesa, CA 92626-1420
USA

For more information, visit:
Ibm.com/software/ecm

IBM Corporation
3565 Harbor Boulevard
Costa Mesa, CA 92626-1420
USA

Printed in the USA

02-12