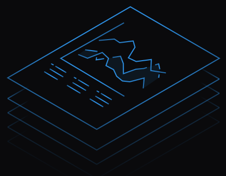
DATA SHEET

Improve Counter-Terrorism Measures with DataRobot



AI for Counter-Terrorism

The DataRobot automated machine learning platform accelerates your AI success by combining cutting-edge machine learning technology with the team you already have in place. The platform incorporates the knowledge, experience, and best practices of the world's leading data scientists, delivering unmatched levels of automation, accuracy, transparency, and collaboration to help your business transform into an AI-driven enterprise.

Internet communities can be fertile ground for recruiters working with terrorist groups. Intelligence professionals must find and analyze information posted on the dark web to detect people either likely to be exposed to extremism or in the process of being indoctrinated to commit violent acts.

This is challenging work. Because it is not indexed, information on the dark web is not accessible from search engines. Volumes of information are vast, as are the number of sites where information is published. Attempting to find and analyze relevant information by human effort alone is an uneconomic proposition.

However, building traditional hand-crafted AI models in the form of machine learning creates two problems. Knowledgeable analysts typically do not have the skill set to code and develop accurate models. Additionally, hiring enough data scientists to solve the problem becomes cost-prohibitive and time-consuming, as it can take over a year to produce a model that is production ready. This is where DataRobot assists:

FOCUS ON RELEVANT AND MEANINGFUL DATA

Artificial intelligence in the form of machine learning models capable of natural language understanding can trawl continuously through enormous volumes of internet data to isolate signals in the noise.

STRATEGICALLY LEVERAGE EXISTING RESOURCES

Automated machine learning boosts the productivity of data scientists already employed by agencies, allowing these experts to build thousands of models in the time it previously took to build just a few.

UTILIZE INNOVATIVE AI METHODS

Agencies responsible for counter-terrorism can construct innovative work practices where AI finds information of interest and forwards this to human experts who work only with relevant information and apply their knowledge and judgment to make decisions that protect the nation from emerging threats.

ENABLE ANYONE TO BECOME AI-DRIVEN

Automation reduces the level of expertise needed to adopt AI. By empowering their domain experts already in service to create machine learning with no programming, the Federal Government can accelerate its path from data to knowledge.

DataRobot, the leader in Enterprise AI, offers automated machine learning capabilities that are simple and safe to put into production, so even inexperienced users create valid and explainable modeling results.

With DataRobot, federal government agencies responsible for countering terrorism can forecast and detect online activity of groups and individuals intent on violent extremism. By building the right model in minutes rather than months, these federal agencies can respond quickly and remain current as criminal tactics evolve, improving the effectiveness and productivity of counter-terrorism professionals.

DataRobot enables counter-terrorism measures in the following ways:

DETECT CYBER RECRUITMENT

Online communities enable violent extremists to increase recruitment by allowing them to disseminate literature and training materials used to build personal relationships with a worldwide audience capable of accessing uncensored content. Machine learning using techniques, such as topic modeling to recognize clusters of words describing violent acts and rewards for participation, can automatically identify forum posts intended to recruit new members. Once detected, potential recruitment behavior is forwarded to counter-terrorism experts for review and action.

FORECAST CYBER RECRUITMENT

Violent extremist organizations do not behave randomly, but instead target forums and time periods in which the online communities appear to be vulnerable to recruitment propaganda. Forecast models can predict the timing of recruitment content. Significant errors in these forecasts (i.e., surprising surges) may be predictive of planning for future operations and can serve as helpful indicators of related illegal activity like money laundering and money transfers to the recruiting organization.

DETECT CYBER RECRUITER

Recruiter behavior may provide important clues for analysts tasked with disrupting terrorist networks. Just as recruiting content can be recognized, the accounts that disseminate recruiting content could be flagged and characterized. Machine recognition of recruiters can help analysts intervene, track, disrupt, and further evaluate recruiter networks.

AI helps staff analyze huge volumes of data with limited resources by developing, testing, and improving predictive models to identify risky patterns and activities. Analysts can identify locations most at risk and individuals most likely to be recruited by terrorist organizations.

Contact Us

DataRobot
1775 Tysons Blvd., 5th Floor
McLean, VA 22102, USA

www.datarobot.com
info@datarobot.com
public-sector@datarobot.com

powered by aws