1:30 p.m. – 2:00 p.m.
Sharpen Cyber Defenses with AI and Machine Learning

Rajiv Shah
Senior Data Scientist
DataRobot

Abstract

Defense, homeland security, and intelligence agencies face an evolving and expanding array of cybersecurity threats. Cyber operations teams must improve their security posture and boost the effectiveness of their cybersecurity solutions and protocols. Applying automated machine learning can help detect threats that have previously circumvented traditional cybersecurity technologies. Cyber warriors don't require coding or data science backgrounds to apply machine learning and develop predictive models to analyze and adapt to new and emerging cybersecurity threats. During this session, you'll learn how cyber operations teams can build stronger, more comprehensive, and proactive cyber defenses by employing automated machine learning technology.

Detailed Description

The volume of data generated by network sensors and security tools is overwhelming already-stressed cybersecurity teams. Additionally, hackers are adept at hiding their tracks and avoiding cyber defenses. This combination of circumstances means the time between breach and discovery is weeks or months, inhibiting the effectiveness of cyber operations teams.

Artificial intelligence (AI) and machine learning helps cybersecurity organizations address these challenges, enabling them to identify patterns of malicious activity in the massive volumes of data. However, there is a shortage of data scientists with the skills and experience necessary to implement AI and machine learning solutions – and even fewer data scientists have cybersecurity expertise, putting the pressure on already-stretched cyber warriors to quickly get up-to-speed with techniques that normally take years to master.

Defense and Intelligence agencies need a new approach. They must predict attacks before they happen, proactively address threats, and leverage the domain expertise of their cyber operations teams. DataRobot's automated machine learning solution makes this possible, constituting an important part of a defense-in-depth strategy. DataRobot enables cyber warriors to prioritize the risks and stay ahead of threats without the need to invest in additional data science talent.

Automated machine learning enables cybersecurity teams to operate on a cyber scale and at cyber-speeds. Predictive models provide insight into network and user activity, uncover the indicators of attacks and compromises, and predict when an attack is likely — all at a speed that is impossible for cybersecurity analysts acting on their own. Automated machine learning makes it possible for agencies to take advantage of predictive analytics to develop and deploy models that identify suspect devices or activities, identify dangerous behavior before a breach, and proactively prevent threats.

DataRobot allows DoD and Intelligence agencies to pull datasets from a variety of sources, running them through multiple algorithms that enable operators and analysts to identify and take action against security threats before they happen. The platform enables agencies to meet mission objectives faster and more efficiently using predictive analytics, with 24/7 access to data wherever it resides – C2S, AWS GovCloud, Hadoop cluster, or on premise so cyber warriors are empowered to quickly make critical decisions.

DataRobot's automated machine learning platform combines predictive modeling expertise and data science best practices to deliver accurate, actionable insights to help cyber warriors combat external and internal threats. DataRobot's models are human-interpretable, giving staff deep insight into the factors that drive the models. Additionally, DataRobot offers a user-friendly drag-and-drop interface that allows cybersecurity teams to quickly develop, test, and deploy predictive models without having to learn new programming languages.

With DataRobot, cyber warriors easily build models that analyze network and user activity, learn and adapt to new threats, and quickly anticipate attacks. Automated machine learning-powered solutions make it possible for any agency to take advantage of predictive analytics to accelerate the modeling process, enabling cyber operations teams to identify threats in minutes or days rather than weeks or months.

Predicting and Preventing Network Intrusions – Endpoint security like firewalls, anti-virus software, and more continually evolve to stop new attacks. In the process, they accumulate data about emerging and sophisticated threats that often bypass traditional signature-based malware detection. DataRobot extends these systems, enabling cybersecurity teams to easily build predictive models that analyze network and user activity, detect patterns in data, learn about and adapt to new threats.

Thwarting Insider Threats – DataRobot addresses insider threats by giving cybersecurity teams the power of prediction to evaluate insider behavior and identify precursors to malicious or risky actions. DataRobot's proactive monitoring, detection, and prediction capabilities provide granular information about who users are and what they are doing so that cyber warriors can immediately respond to risky data access and contain the threat before damage is done.

Elevating Cyber Operations Staff – DataRobot accelerates the cyber defense teams' ability to do what it does best: create intelligent and effective solutions to new threats. By combining human intelligence and domain expertise with machine learning technology, cyber operations teams automate the discovery of new attack methods, allowing them to quickly connect the dots, devise new defenses, and strengthen their response. DataRobot's automated machine learning technology flags high-risk activity, freeing up valuable cybersecurity experts to focus their attention where it matters most and avoid chasing false positives.