How Government Agencies Can Level the Cybersecurity Playing Field With AI/ML

By Dr. Sarbari Gupta, Founder and CEO, Electrosoft Services, Inc.

The threat cybercriminals pose to federal information systems and networks is real and pervasive. Defending against unauthorized intrusions is a full-time effort for federal agencies and the contractors that support them. Complicating the effort, today's cyber resilience is both challenged and bolstered by artificial intelligence and machine learning, with cyber defenders and cybercriminals vying to gain the edge.

Harnessing AI/ML for Early Threat Detection and Defense

In cybersecurity, early detection is paramount. AI, with its rote task automation and round-the-clock availability, offers speed and algorithmic precision in evaluating large amounts of data. It can also identify suspicious activities, behaviors, and even zero-day attacks. Its pattern recognition capabilities surpass those of human analysts, adding to AI's early detection credentials. Moreover, AI's capability to distill and analyze data can better separate "real" threats from miscues or lower-priority issues, sparing analysts from this time-intensive task and allowing them to focus on critical events.

AI can counter a relatively new and impressive threat: the bot. Beyond expected actions (bot recognition and blocking), AI offers enhanced security features (e.g., stronger captchas) and the capability to create honeypots that attract bots and allow analysis of their functioning in controlled environments. AI and ML also shine in their capacity to recognize and detect new malware variants based on experience with earlier versions.

Speedier detection allows IT staff to quickly institute defensive measures. Additionally, AI can undertake defensive action on its own. As an example, AI can redirect system traffic to unaffected servers. Also, AI can block suspect IP addresses and incoming emails believed to contain phishing schemes as well as close compromised accounts.

AI for Proactive Cyber Resilience

AI can function in proactive ways, too. It can scan systems and identify vulnerabilities in need of strengthening. Additionally, it can automate system functions, such as patch management, to ensure software vulnerabilities are remedied quickly.

AI heightens secure authentication measures which, if undermined, offer a common gateway into systems or networks. AI allows multifactor authentication, whereby systems can request and process in real time something you know (password or PIN), something you have (PIV card or token), or something you are (biometrics such as a fingerprint). AI elevates this triad by detecting patterns regarding when a user typically logs on, the device most often associated with the user, the locale from which logon occurs, and so forth. When changes in these patterns occur, it can signal an effort to gain unauthorized access.

Last, but not least, AI/ML offers predictive forecasting capabilities. The same features that discover suspicious activity and unusual behavior patterns can warn analysts of events that could be indicative of a future attack. Knowing that something nefarious may be afoot enables an organization to boost defenses and institute other preventive measures. Of course, it is not an exact science but, as the adage goes, “An ounce of prevention is worth a pound of cure.” Attacks can be devastating and expensive in terms of organizational disruption and the costs of system software and hardware as well as data recovery and forensics.

Prediction capabilities increase when AI and natural language processing work in tandem. By drawing on sources such as the Cybersecurity & Infrastructure Security Agency Cybersecurity Alerts & Advisories, as well as other information sources such as studies, news articles, and the like, AI tools increase their capacity to discern the latest attack precursors and prevent them.

Cybercriminals Are a Step Ahead

Cybercriminals seem to have untold resources, some derived from the sponsors of their crimes and some from their victims. Safe to say, most organizations don’t possess the same deep pockets or the learning opportunities that a life of crime offers, giving cybercriminals an advantage.

Attackers are continually creating new bots, new malware, and honing their phishing attacks. In addition, use of AI to create deepfakes is a potent weapon on many levels, motivating individuals and organizations to take action due to non-reality-based audio and video. Here, AI is at once the creator of criminal tools and the executor of the crime.

AI currently appears to afford cybercriminals greater advantage. So, how can we turn the tables on these malicious actors?

Leveling the Playing Field with AI/ML

Many organizations desire strong cybersecurity, but such an objective is resource-intensive in terms of the budget needed to support personnel, equipment, and other tools. One key to cyber resilience is moving toward digital transformation and modernization, incorporating the cloud and zero trust architectures. Another is the adoption of AI and ML to help level the playing field through automation.

Federal agencies are on the right track in the AI realm. The opportunity is to do what they're doing now, even better:

- Advanced Identity, Credential, and Access Management approaches
- Enhanced forecasting and prediction models
- Better pattern recognition algorithms
- Augmented risk identification and management capabilities
- And more …

Combined, these advances – and those we can't even imagine today – will offer the resilience necessary to switch the advantage to our cyber defenders.

About the Author

Dr. Sarbari Gupta is the Founder and CEO of Electrosoft Services, Inc. She is a recognized thought leader and speaker on cybersecurity, zero trust, ransomware, ICAM, FIDO passkeys, OSCAL and more. She is an active NIST collaborator and co-author, helping to shape cybersecurity standards and guidelines to improve federal cyber resilience. 2022 was a banner year for Electrosoft, with record revenue and 25% Y/Y growth – and the company is on track for 60% growth in 2023. Dr. Gupta is passionate about STEM education and encouraging women to embrace and stay in STEM fields. She serves as a mentor for Women in Technology (WIT) and is a member of the board of advisors for University of Maryland Women in Engineering (WIE), providing support and mentoring to women entering an engineering field.

Dr. Gupta can be reached online via LinkedIn and at our company website https://electrosoft-inc.com/.