INFOSEC

Machine learning and AI

AI and machine learning and their uses in cybersecurity

March 31, 2020 by **Rodika Tollefson**

Share:

Artificial intelligence and machine learning trends

Although artificial intelligence and its subfield of machine learning have been applied in cybersecurity for some time, the speed of adoption is now accelerating. As threats evolve and IT environments get more complicated, AI-driven technology shows the potential of addressing new threats and risks that require machine speed rather than human speed.

More vendors are folding machine learning and other AI applications into their solutions — not surprising, considering organizations are increasingly turning to this technology to help stay ahead of threats. Asked by an Oracle survey what the most significant benefit of autonomous technologies was for organizations, "improving security" was one of the top choices by C-suite executives.

In a 2019 survey by Capgemini Research Institute, 69 percent of the surveyed security executives and leaders said they didn't believe they could respond to cyberattacks without AI. Additionally, nearly two-thirds said they were testing AI use cases and almost half said that FY20 budgets for AI in cybersecurity would increase by nearly a third.

In this Series

Related Bootcamps

Below are just some of the ways that organizations can use AI and machine learning for cybersecurity.

Identifying anomalies in network traffic or user behavior

Cisco forecasts the global number of internet users to grow from 3.9 billion in 2018 to 5.3 billion by 2023, a 6 percent compound annual growth rate (CAGR). But what's more mind-boggling is the fact that the number of connections and devices is growing even faster, at 10 percent CAGR. By 2023, the number of devices connected to IP networks will be more than triple the global human population.

As the traffic grows, detecting anomalous behavior in the network becomes more challenging. AI and machine learning (ML) can identify deviations from normal patterns faster, recognizing behaviors that indicate potential threats.

Likewise for users, AI/ML can analyze the data stream for suspicious activity that may indicate an insider threat, such as downloading large amounts of data or repeatedly attempting to access unauthorized resources.

As John Burke of Nemertes Research writes in TechTarget, "Spotting anomalies in network behavior can help cybersecurity teams find everything from a compromised hardware node to an employee going rogue on the company network."

Detecting online and other fraud

Only about 13 percent of organizations surveyed by the Association of Certified Fraud Examiners said they used machine learning to identify fraud, but the amount of money they planned to invest by 2021 will triple. One use case is ML algorithms combing through large data sets such as historical data to find patterns much more effectively than rule-based methods, which can be subverted by cybercriminals.

For example, supervised machine learning would be fed the historical data to determine what fraudulent activity and accounts look like compared to normal ones. Then the model would make a decision based on the account activity and features. Conversely, an unsupervised model could be used when there are few or no "tagged" (or identified) transactions, such as in cases of new types of fraud.

"By choosing an optimal blend of supervised and unsupervised AI techniques, you can detect previously unseen forms of suspicious behavior while quickly recognizing the more subtle patterns of fraud that have been previously observed across billions of accounts," writes TJ Horan on the FICO blog.

Protecting endpoints

CISSP

Security+

Ethical Hacking

CISA

A 2018 Ponemon/IBM Security survey found that endpoint containment was the second most common answer to the question of how AI improves the security posture. More than 60 percent of the surveyed IT and security practitioners said the biggest benefit of AI was containment acceleration of infected endpoints, devices and hosts.

Rapid containment of a compromised host could mean the difference between a failed cyberattack and a full-blown data breach. As one example, machine learning techniques could help identify malicious application behaviors from legitimate ones and stop a file from executing — essentially stopping an attack in real time.

As IBM Security's most-recent annual cost of data breach report noted, "the faster a data breach can be identified and contained, the lower the costs." The report found that the average time to identify and contain a breach in 2019 grew to 279 days (from 266 in 2018). However, breaches that had a life cycle of under 200 days cost $1.22 million less on average than those that took longer than 200 days ($3.35 million vs. $4.56 million).

Mitigating the cybersecurity skills gap

The cybersecurity talent gap continues to widen, impacting organizations' ability to fill vacancies — and consequently defend effectively against threats. Among other things, AI/ML can play a role in mitigating the shortage by enhancing the abilities of a security team and automating threat analysis and response.

One area that could benefit is the security operations center (SOC). In its 2020 CISO Benchmark Study, Cisco found that 42 percent of respondents suffer from alert fatigue, driven in large part by a large number of security solutions they have in place.

For a SOC analyst, cutting through the noise to triage alerts is time-consuming since humans are simply not wired to process large amounts of data efficiently. Machine learning and automation can significantly scale this process.

BlackBerry CTO Charles Eagan put it this way in an interview with VentureBeat: "AI and automation are more about scalability, as opposed to plugging specific skills gaps … if we remove 99 percent of the cyberthreats automatically, we can spend much more quality time and energy looking to provide security in deeper and more elaborate areas."

What to expect next

Organizations will likely leverage AI-powered techniques more and more with time. On the other end of the spectrum, threat actors are also using machine-based attacks to increase the speed and effectiveness of their attack execution. From deepfakes to AI-powered malware, this trend will grow, which means the security community will need to find new ways to keep up.