Essay

Rising Role of Artificial Intelligence in Cyber Security

Durga Prakash Devarakonda

With advancements in research on Artificial Intelligence (AI) due to availability of cheaper computing and storage power from cloud providers, it is increasingly playing an important role in Cyber Security. The next generation of cybersecurity products are actively incorporating Artificial Intelligence (AI) and Machine Learning (ML) technologies. By training AI software on large datasets of cybersecurity, network, and even physical information, cybersecurity solutions providers aim to detect and block abnormal behavior, even if it does not exhibit a known "signature" or pattern. Experts anticipate that, over time, companies will incorporate ML into every category of cybersecurity products.

Artificial intelligence, which includes neural networking, machine learning, analytics, and the use of algorithms to complete tasks, allows machines to learn from experience.In cybersecurity, the machine learning subset of AI has the most use -- at least at this stage in AI development. While there is little use of 'true' cognitive AI, machine learning can provide a springboard from traditional, signature-based antivirus and cybersecurity solutions to a more extensive means of protection through data collection and analysis. When machine learning systems are given a large enough data pool to digest and analyse, they can be used to help shrink attack surfaces through predictive analytics, the detection of what is likely to be suspicious behaviour, and this, in turn, eases the burden on cybersecurity staff who often have to triage cybersecurity-related events on a daily basis. AI and machine learning are not perfect and cannot be considered a silver bullet for cybersecurity defence. However, solutions and platforms which leverage

Dr. Durga Prakash Devarakonda is the Chief Executive Officer of Clairvoy Analytics Private Limited.

these technologies can give the enterprise an additional way to defend itself against cyberattacks which are constantly evolving and increasingly sophisticated.

Threat Detection

There are different approaches to using AI for cybersecurity, and it is important first to determine which is appropriate for an organisation. Some software applications analyse raw network data to spot an irregularity, while others focus on user/asset/entity behavior to detect patterns that deviate from normal. The types of data streams, how they are collected, and the level of effort needed by analysts all vary by approach. Cybersecurity solutions utilising AI and ML can greatly reduce the amount of time needed for threat detection and incident response, and are often able to alert the IT staff of anomalous behaviour in real time. These technologies also help reduce and prioritise traditional security alerts, increasing the efficacy of existing investments and human analysts.

Cybersecurity solutions utilising AI and ML can greatly reduce the amount of time needed for threat detection and incident response…

Attackers are also using AI and ML to better understand their targets and launch attacks. AI increases the ability of defenders to identify attacks, but it may also help hackers learn about a target's vulnerabilities. Cybersecurity product companies have turned to AI and ML to provide insights that would otherwise be impossible for humans to achieve alone. These products use AI to identify anomalies, speed up detection, and increase the effectiveness of existing products. AI can aid analysts who may be overwhelmed with security alerts to identify patterns that may indicate a threat that would otherwise be missed by conventional cybersecurity software. Without this help, analysts can waste time researching "false positive" alerts and researching dead ends, while missing legitimate malicious activity. Organisations can waste as much as US $1.3 million per year responding to "inaccurate and erroneous intelligence" or "chasing erroneous alerts," according to a study conducted by a large non-profit security organisation in United States.

Better solutions are obtained by using ML to analyse vast stores of human-labeled data so that it can find patterns within the noise. For as long as ML has existed, training has been the most lengthy and cumbersome part of AI/ML implementation, but several AI solutions have now been developed that permit the software to train itself autonomously, at least in part. Given proper training, AI threat analysis can apply human-

like intuition to every interaction on the network and pluck a single strange packet from millions of others for human review. Some AI products on the cutting edge allow companies to correlate attacks or events across time and geography to develop a better picture of what is happening within the network. When properly monitored, solutions that detect threats using ML can reduce the time from breach to discovery, reducing the amount of damage an attacker can cause. Shortening the time to discovery is critical for security, especially because the average breach can still take over 260 days to be discovered.

Different Approaches

Different AI/ML approaches can be used for different security objectives. In one approach, AI software looks at raw network activity data to flag any unusual connection that is being made, e.g., a packet comes into a SCADA network from an unknown IP address. This is basic pattern spotting, and is fairly rudimentary. Alternatively, defending against a threat actor using compromised legitimate network credentials moving slowly through the network or an insider threat may require deep learning to analyze a given user's behavior over a series of actions to determine if the pattern of behavior is out of the ordinary. This approach is what is known as behavioural user analytics. In this system, the AI is implemented at the user/asset/entity-level to surveil an employee's or device's activities, e.g., an employee accesses a local server that they connect to infrequently, and then begins downloading all of the server's contents. In either the former or the latter case, the AI will recognize that there is an anomaly and will alert IT staff for further investigation. Behavioural user analytics is quickly becoming the gold standard for cybersecurity products in the AI domain. Artificial Intelligence-Machine Learning driven Packet data capture Analytics will give more precision threat detection, hunting and prevention capabilities to enterprises.

An important aspect for an AI platform is transparency in the decision-making process. This is important for instilling trust among those that use it or are subject to its calculations and decisions. AI threat detection software is a black box whose machinations cannot be understood. Explainable AI is going to be more acceptable by industry. Enterprises are keen to understand AI Bias and log file for each of the bias. The software will be more accurate and an organisation more secure if users know how to gauge if the AI is right or wrong, making user feedback much more useful. For companies that do not have large cybersecurity or IT budgets, an AI platform sifting through

hundreds of gigabytes of network activity data on a daily basis can be as effective as several teams of IT staffers using conventional tools for threat detection.

Unfortunately, AI is already being used for nefarious ends by hackers and other cyber criminals. In 2016, an experimental AI was employed to send simulated spearphishing links to Twitter users to determine how effective it could be when compared to a human performing the same task. Though the AI only lured 34.4 percent of its targets to the fake phishing websites compared to 38.0 percent for the human, the AI was able to churn out over 800 attempts compared to the human's 130 attempts in the same amount of time. This illustrates that even if an AI is less effective at tricking people than humans are, it still undoubtedly has a massive speed advantage, allowing it to "cover more ground" than a human and, in the end, create more victims. The Twitter phishing experiment is perfectly analogous to AI's primary use case for cybercrime, whereby threat actors employ the automated advantage that is inherent in system. Whether it is DDoS attacks, ransomware, or some other kind of malware, cyber criminals are using AI to spread the threat faster and target more vulnerable machines.

The Cyber Security Industry is moving very fast in terms of applying various aspects of Artificial Intelligence for betterment. Some of the well-known firms started accepting in this area are Symantec's Targeted attack analytics (TAA) tool, Sophso's Intercept X tool, Darktrace's Antigena, IBM's Q Radar Advisor and Vectra's Cognito. Applied AI in cyber security is at very early stage and there is lot to do. The adoption of AI can have a very positive impact on an organization's security posture and bottom line. The biggest benefit is the increase in speed of analysing threats followed by acceleration in the containment of infected endpoints/devices and hosts. AI reduces the time to respond to cyber exploits, large organisations can potentially save an average of more than US $2.5 million in operating costs. In addition to greater efficiencies in analyzing and containing threats, AI identifies application security vulnerabilities. In fact, AI increases the effectiveness of their organisations' application security activities.

Using anomaly detection and machine learning, AI will hugely disrupt the field of Cyber Security.

AI and Cyber Security

The last key trend in the exponential technologies space for 2019 pertains to cyber security. While this is a remarkably advanced field, we will see continued growth and evolution of cyber security in combination with Artificial Intelligence. Using anomaly detection and machine learning, AI will hugely disrupt the field of Cyber Security.

Security practitioners will be empowered to identify intrusions and malafide behaviour faster using the automated, always-on algorithms to constantly survey the secured network for wrongful activity and address concerns before they break-ins occur. AI can quickly sift through the massive data set of a cyber security network, and even physical information. Cyber Security vendors will soon roll out AI-Enabled solutions that will learn at an abstract level to detect and block abnormal behaviour, even when this behaviour does not fit within a known pattern. It is expected that in 2019 companies will incorporate ML into all categories of Cyber Security Products.

By extension, we will see a fight between good AI and bad AI in the domain of Cyber Security. There are genuine fears that the next generation of attacks will not be carried out by human hackers but pieces of code designed to rapidly infiltrate a secure environment. Countering that with so-called "good AI" will be crucial in undermining the impact these fast-paced attacks can have.