AI: An Intelligence Artificially (almost) Human

Ramsés Gallego

CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt

Security, Risk & Governance International Director, Micro Focus

The developments in Artificial Intelligence (AI) represent a giant leap in the way of approaching complex problems that require capabilities beyond human ability. After all, already at the time of the industrial revolution, machines were developed to expand human effort, to amplify the qualities - at that time physical - of the labor force. In our hyper connected digital, technological age, machines (*read algorithms*) are aimed at increasing our analysis speed and multiplying the possibilities of inferring information and making more agile decisions. Trust me, I don't know of any cybersecurity analyst who can deal with massive amounts of data, hundreds of thousands of sources of information per second… but I do know of a few algorithms that can do (and they do) so as a result of their daily 'work' (a concept that deserves an article on its own for the ethical and social consequences of it al).

It is important to highlight that Artificial Intelligence is the 'supra-discipline', the umbrella that contains five sub-disciplines, one of them being the best known, Machine Learning.

This dimension, clearly the most applied in the field of cybersecurity, has, in turn, four modalities that deserve explanation: Supervised, Unsupervised, Reinforcement Learning and Deep Learning. Although it is true that each one has its particularities and I could develop (almost) a book about them, for the purpose of this article - the application of all this in cybersecurity - I will focus on two: Unsupervised and Reinforcement Learning.

The first one, Unsupervised Machine Learning, does not require a data scientist to 'label' the data set and the algorithm is capable of 'automagically' (*sic*) deciding the variables that you need to test the hypothesis as correct or incorrect. This modality is ideal for finding anomalies, behavioral patterns and, thus, being able to even infer the next movements of the attacker and/or any individual in the community. Unsupervised Machine Learning is the most widely used at the moment due to its ability to predict using volumes of information from different sources, with massive data loads, in (almost) real-time and making very deep use of statistics.

With Reinforcement Learning, as its name suggests, the algorithm is capable of learning from its mistakes (!) and learning intensively, correcting its state and always being in the best version of itself (which, as a concept, it is already extremely interesting because it implies that it is in continuous improvement mode ... always). In the world of cybersecurity, applying this concept to defense strategies where the machine can learn from its mistakes and (re) learn from, for example, false positives, seems to us a qualitative and quantitative leap. Can you imagine a solution that can predict the next step of an attack... because it has been trained and/or seen different methods to exfiltrate information (what is known as TTP, Tactics, Techniques and Procedures) and act accordingly even before it happens? Stop imagining because that already exists and substantially changes human efforts in protection and defense in cybersecurity.

At Micro Focus we pride ourselves on having Machine Learning technology that completes and complements existing developments in obtaining full control and visibility of the environment. Our engineers have developed detective, preventive and corrective controls with our Interset technology that capitalizes on the concepts mentioned in this article. And they provide new angles for the deployment of a new generation SOC (Next-Gen Security Operation Center). An automated, orchestrated SOC that is capable of using threat intelligence from a variety of sources (including multiple data lakes) inferring the next step of a cybercriminal, and consequently bringing greater robustness and robustness to protecting and defending an environment.

All this, before arriving at Deep Learning, whose conceptualization aims to emulate how the human brain works, the way in which the one hundred billion neurons estimated to have the brain of an adult work in different layers to pass information and take decisions in the very same way our brains sends electromagnetic impulses or electric currents. So we live in a fascinating time in cybersecurity where tools enlarge human capacity. We live in a magnificent time where artificial intelligence is less and less artificial and more intelligent. Less and less machine and more human. Or almost.