1-2021

FireEye: Cybersecurity in action

Singapore Management University

Citation

Singapore Management University. FireEye: Cybersecurity in action. (2021).
Available at: https://ink.library.smu.edu.sg/pers/563

FireEye: Cybersecurity in action

29 Jan 2021

FireEye built its success on its 'Human + AI' philosophy. But can a cybersecurity firm get ahead of the attackers and predict an attack…on itself?

In the space of nine years between 2010 and 2019, cyber security firm FireEye has grown its revenue from US$11.8 million to US$889.2 million. The secret of its success was its conceptual AI framework called the 'Automatibility Spectrum', which determined the appropriate degree of automation for developing different solutions. Repetitive tasks were performed by automated algorithms while decision-making involved human verification.

Machine learning (ML) techniques were used to reduce the time to discover and distribute threat intelligence, as well as generate efficiencies across its product and services offerings. This required constant refining, an approach whose benefits were not always immediately visible and which needed a mind-set shift in human analysts to trusting a model's findings in their analysis.

On December 2020, FireEye posted on its blog news of a "highly sophisticated state-sponsored adversary" stealing its Red Team tools, which are technology and techniques used by security professionals to mimic potential cyber security attacks. Defenders aka 'Blue Team' demonstrate how these attacks can be stopped.

If cyber security specialists such as FireEye can be hacked, are defenders doomed to fight rearguard action instead of building stronger defences? Given the long gestation period of AI solutions, how could FireEye could deliver its expertise seamlessly with the help of AI tools, arming human experts with the exact information they needed, when they needed it most? Was the Human + AI approach the right strategy for FireEye?

HUMANS + AI = CYBER SECURE

At FireEye, AI solutions, including machine-learning based methods, had been implemented for a variety of applications including malware detection and antivirus support, malicious PowerShell detection, tools for email monitoring and phishing attack detection, as well as a variety of tools to support internal staff doing security operation centre analysis, incident response, and reverse engineering.

When used in conjunction with human expertise, it had the potential to deliver effective cyber security that kept up with ever-evolving threats.

"In cybersecurity, the biggest challenge is the skills gap," explains **Steve Ledzian**, Chief Technology Officer of FireEye Asia Pacific. "We do not have enough human analysts to do everything that we want to do. AI/ML tools help analysts to take away some of those very tedious manual tasks that they are required to do, so they are freed up to do higher order tasks that require expert human decision-making skills. The tools also help prioritise what human analysts should focus on.

"ML is one of the useful tools in an array of products. We have quite a wealth of data; in ML data is very important, but available datasets have to be kept up-to-date. Making sure that the right data is fed into the model is important, as the quality of the analysis critically depends on the quality of data."

For a cybersecurity firm, the ongoing need for model updates due to the regular appearance of new vulnerabilities always led to the risk that the changes could have negative interactions with the cybersecurity infrastructure and related workflow, which threatened to reduce an ML model's value. FireEye had chosen to invest a great deal of managerial attention and technical expertise to balance this inherent trade-off between constantly making changes to ML models to incorporate updates and managing the risks associated with making those changes.

A key aspect of the human + AI approach adopted by the FireEye AP team was that it tried to consciously keep such technical debt in check, by moderating the extent of the dependency on the model and having a layer of human support and intervention (much like a school teacher keeping an eye on a student's learning), and intervening to correct the understanding wherever applicable.

A GAME OF 'CAT AND MOUSE'

Cybersecurity was like a never-ending competitive 'cat and mouse game' between the legitimate protectors and the criminal attackers. And sometimes the protectors became the attackers. What was clear was that the entities (whether they were the "good guys" or the "bad guys") that could move at greater speed and larger scale to make use of data to amplify their learning and intelligence would have the advantage, and would ultimately prevail.

With the theft of its Red Team tools, many questions have been raised: Could FireEye create a winning source of tools and models to keep up with—or better yet—keep ahead of the attacking opponent every time? Did AI really hold the key to the future of cyber-security? Was its existing approach, a symbiosis of human capability and AI-enabled machine support, the right way forward?

Could FireEye raise the bar and develop predictive AI tools that could foretell what a threat entity would do in the future? Could FireEye build a Predictive Analytics solution to predict the next cyber-attack, perhaps even one targeting itself?

This is an adapted version of the SMU Case, "Cybesecurity at FireEye: Human+AI". To see the full case, please click on the following link: https://cmp.smu.edu.sg/case/4736".

Follow us on Twitter (@sgsmuperspectiv) or like us on Facebook (https://www.facebook.com/PerspectivesAtSMU)