APSM | ASIA PACIFIC SECURITY MAGAZINE

http://www.asiapacificsecuritymagazine.com/artificial-intelligence-cybersecurity-scaling-up-for-the-internet-of-things/

Artificial Intelligence & Cybersecurity – Scaling up for the Internet of Things

26/09/16

By APSM on Sep 26, 2016 in Asia Pacific Security, Cyber Resilience, Editors Desk, Featured, Security Products, Spotlight on Security, TechTime

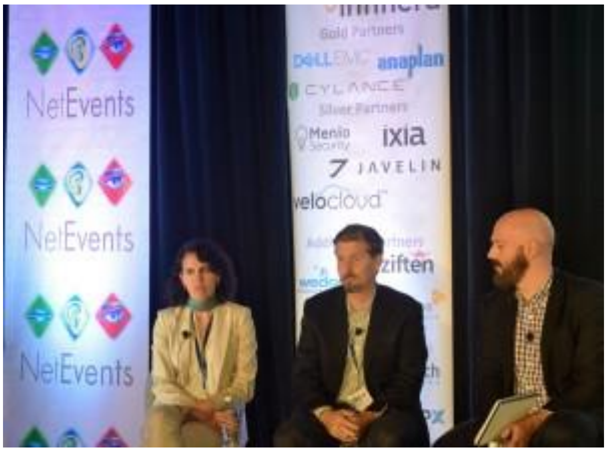
The Internet of Things – 2020

$1.46 T Market Opportunity

IoT Market Opportunities: Source IDC

The world may only get one chance at making IoT, the Internet of Things, actually work. No one knows where this technology is ultimately headed. Had the Internet's originators in the early 1960's taken a glimpse into the year 2016 and attended last week's NetEvents IoT and Cloud Innovation Summit at Saratoga's Mountain Winery, a relatively short drive from the Stanford Research Institute (SRI) where the first Network Working Group meeting was held in 1968, I wonder how different the Internet may have been or how shocked they would be at the machine they have unleashed.

We know that the Internet lacks 'security by design' and hence why security remains the fundamental element of how we safely enable the unfolding IoT revolution. According to Dr. Glenn Ricart of USIgnite, a not for profit organisation born from the White House Office of Science and Technology Policy and the National Science Foundation, "we are entering the time when we take the Internet away from humans and hand it over to machine controlled 'things'."



NetEvents 2016 opening panel discussion – Kathryn Hume, Stuart McClure and Ovum's Paul Jackson

Kathryn Hume heads up Fast Forward Labs, a specialist advisory firm operating across a range of industries including insurance, publishing, finance, media, and government on data product development, technology, and culture. Kathryn opened the two-day program by walking through the work they've done in natural language generation and deep learning in image analysis and text summarisation. As Katheryn impressively noted – the real impact of today's technology lies in 'making complex data simple' and how the focus needs to extend beyond just the hype and find true, but often hidden value. There is a long way to go.

One shining light being shone on the security dilemma though is the application of Artificial Intelligence (AI) and how it is applied to solving the security challenges of today, and hopefully tomorrow. There are between 5 to 10 start-up companies being created each week in Silicon Valley, California within the domain of AI and each focusing on the almost limitless applications across every industry.

Stuart McClure, founder and CEO of Cylance, has moved security applications to beyond programming and in what is hyped to be a game changer, is teaching security systems to predict, prevent and detect cyber threats. Similar somewhat to the early application of actuarial science, Cylance is applying AI in the form of pre-execution algorithms to prevent, detect and respond to malicious code and anomalous online behaviour.

As McClure points out, "if it's blocked we don't care and if it's not blocked we want to understand why it wasn't blocked." Then Cylance sets to replicate and improve, training itself to look automatically and instantaneously for features that are going to be indicative of being good, bad and in between, and using millions of signatures, features and behaviours to initiate unsupervised learning and then move to supervised learning of all known clusters of bad profiles and continue to extract features and classify between good and bad.

The approach is to build security systems to achieve prevention to 99% and the 1% they can't prevent they want to detect 99% of the 1% and then develop the response to 99% of that 1% – and so on. Sounds straight forward and as this approach is applied on a massive scale, it is understandable why Cylance has emerged as one of the most effective cyber security companies on the internet. "Without AI, we can't possibly scale to meet the demand" McClure asserts. But even at full scale in the Internet of Things – is 0.0001% risk, or an adversary's opportunity, enough to cause a major catastrophe?

To understand how AI is being applied, anyone who has raised children or trained a dog to fetch a ball will understand the concept. Kathryn and Stuart’s opening discussion helped simplify the requirements. “An average person will need to see three cats and be told each time it’s a cat before they will recognise a fourth cat, but for AI, the computer needs 50,000 cats to start to recognise a cat. But accessing the data, CPU power and bandwidth is getting better and therefore so will AI.”

When Cylance is applied to 100,000 node networks the system immediately starts detecting and then reverse engineering existing malware attacks. Most traditional systems are detecting 40% compared to 99% for Cylance and the closest competitor has only achieved 52%. So the choice appears clear. Despite my initial hesitations to the application’s market take up, Cylance is making rapid and significant inroads, with Series D funding raising around $100M, taking it to a total of $177M. Current valuation is believed to be at US$1.2B – putting Cylance into the unique ‘Unicorn’ category.

The most recent announcement has been from Wedge Networks, and the newly released Wedge Advanced Malware Blocker, or WedgeAMB, the first product in the Wedge Absolute Real-time Protection (WedgeARP) series of enterprise solutions. The WedgeARP series provides fully self-contained, security platforms in the form of virtual machines that orchestrate real-time hyper-inspection engines. WedgeAMB applies Cylance’s AI technology to detect and block viruses and advanced malware, such as ransomware, at the network level, preventing them from entering enterprise networks. The combination of Wedge’s hyper-inspection with Cylance’s machine-learning engine and WedgeIQ threat analytics, WedgeAMB promises to be a break-through in malware prevention.

According to the Federal Bureau of Investigation, ransomware is on the rise in 2016, with one group estimated to have been paid over US$120M in just 6 months. Ransomware-as-a-service is now also available. Advanced malware and ransomware attacks also account for millions of dollars in lost productivity and theft by cybercriminals operating on a global scale to exploit endpoint devices with increasing levels of sophistication. Unless solved, this malicious activity will put IoT at serious jeopardy of being hijacked before it begins.

With millions of cyber-attacks occurring daily on networks around the world, cybersecurity seems the perfect area to apply AI. There remains just three key methods to a cyber-attack – denial of service to cause failure, execution based attacks and authentication based attacks. “AI can be applied to all three in a very meaningful and effective way”, but as McClure notes further, “you just need the data and we are a long way from automatic classification in AI”. As we come to understand where this technology will take us, the battles will continue, as the IoT revolution unfolds alongside the growing sophistication of attackers. We are yet to see where this all takes us but it will be an exciting journey nonetheless.

Chris Cubbage, Executive Editor