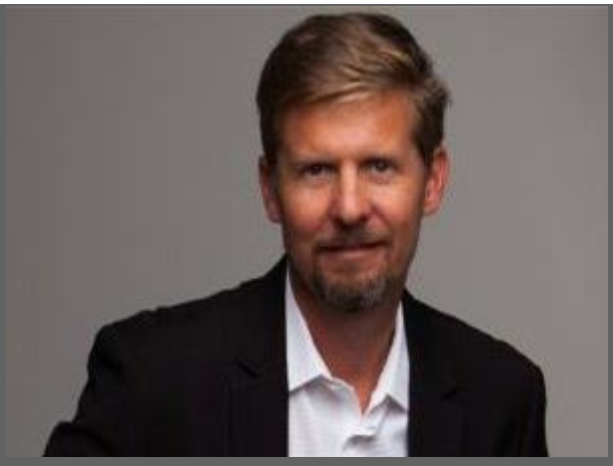
http://www.itweb.co.za/index.php?option=com_content&view=article&id=156043

# Using AI to fight cyber crime

22/09/16

By Sibahle Malinga, ITWeb's portals journalist.

California, 22 Sep 2016

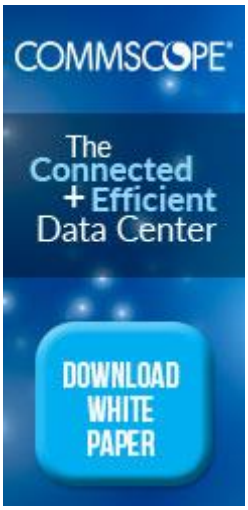


Using antivirus software built on artificial intelligence and machine learning is one of the most effective ways to detect and prevent cyber attacks, says Cylance's Stuart McClure.

There are around 350 000 to 400 000 new cyber attacks occurring every 24 hours globally. In order to effectively fight cyber crime, organisations need to learn to apply artificial intelligence (AI) through software that predicts and blocks attacks on the end-point in real time, using pre-execution algorithms.

This was according to Stuart McClure, CEO and founder of security company Cylance, speaking at the NetEvents Global Press and Analyst IOT and Cloud Innovation Summit held in California, US this week.

McClure pointed out that AI is one of the most successful techniques used to prevent attacks through predicting how malware, zero-day attacks, and other cyber threats attack networks, with the ability to block up to 99% of new attacks.




"Using antivirus built on artificial intelligence and machine learning to predict cyber attacks involves creating a repetitive pattern of threat behaviour and a replication of detection capabilities. There are over 5 million detection features which are indicatively defined as either malicious or safe. The algorithm is trained on what is classified as good and bad binary files, it then automatically detects features which are going to be indicative of either good or bad behaviour," he noted.

McClure believes the more data you give a learning algorithm, the smarter it will become and the more it will create a distinction between good and bad files.

**See also**

- SA firms lose R28.6m to data breaches
- Espionage key reason for mining cyber attacks
-
- **Cyber criminals**
- **cyber attacks**

"AI can be applied to detect and prevent denial of service attacks, execution-based attacks and authentication based attacks. There are three ways to address cyber security: Through preventing the attack, detecting the attack and through responding to an attack. Organisations should push the focus onto prevention rather than responding to attacks as quickly as they can.

"In a situation where organisations build a prevention programme that can prevent 99% of attacks, the 1% which they cannot detect will eventually catch up with them months or years later, and then they would be forced to respond to the attack. The 1% which they cannot prevent should at least be detected 99% of the time," he asserted.

Some traditional techniques used by most organisations to detect malware, he continued, include signature-based technologies such as antivirus, which monitor certain behaviour or malicious activity which has occurred in the past. This often comes with many loopholes, he warned.

"The problem with this method is that it requires someone to get hacked first, before it is trained to detect this behaviour, thus learning from the victims' past experience. With AI you no longer need a previously hacked victim before knowing that certain behaviour is malicious.

"Supervised learning algorithms are about training systems based upon decisions that human beings have made in the past and automating those decisions. In the early days of learning how to program a computer, we controlled the software by telling it how to do things and it would respond. However today we teach the computer to learn what we will be programming in future, which is usually done in many industries but not often enough in cyber security," concluded McClure.