Is AI Changing IT Security?

Artificial Intelligence

Artificial Intelligence will it really change the way we manage IT security or is it just a marketing phase?

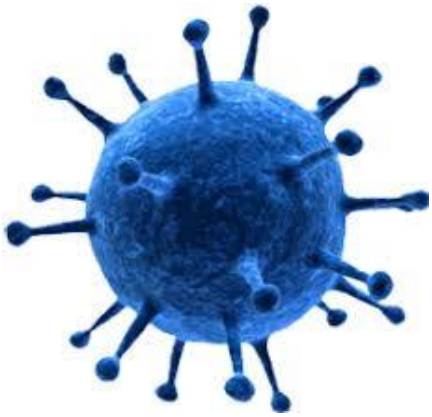
Michael Demery
Managing Director, Seccom Global

What thoughts go through your mind when you think of Artificial Intelligence (AI)?

Do you envisage a Hollywood movie scenario where robots have devastated the earth and have now taken over? Not sure we are there yet - but AI is here, and while we are barely scratching the surface of its many applications, it is making a difference to almost every facet of our lives, and in particular the IT Security landscape. The following paper will look at why traditional methods of securing our business information assets may no longer be effective enough and how new technologies such as AI will likely be essential to IT Security moving forward.

It is important to understand that the network perimeter, once generalised as the area that sat between the public internet and our organisation's own internal network, was once reasonably uncomplex and relatively easy to secure. The adoption of public cloud services and a more mobile workforce expanded the attack surface changing the traditional definition of the perimeter. This change required us to adapt and more consideration was needed to ensure our networks remain secure. We had to think beyond the traditional and design new methods to address the shifting landscape. In addition to the changing attack surface, the amount of data we now create (and store) is exponentially more than any time in history. It is estimated 80% of the worlds data has been created in the last few years.

To understand why change is required we need to understand the change in the data we are now creating. The increase in users and devices now utilising the internet means an exponential increase in unstructured data - data that is not organised in a predefined manner. It is estimated more than a billion new users will be on the internet in the next few years and more than a trillion dollars will be spent on the Internet of Things – IoT. In conjunction with this, social media, unified communications, business to business collaboration and a more mobile workforce will create even more unstructured data. We need AI, with its ability to consume copious amounts of data and identify anomalies faster than we can.



The recent pandemic, experienced worldwide, looks to have changed how we will operate moving forward. Although no one can ever accurately predict what the future will look like, many experts agree that it will be very different post-pandemic. What we do know is that the security component to any solution is always playing catchup to development and any fast-paced change creates challenges.

As an example, consider how we manage software today and how this has evolved as technology and connectivity has evolved - not so long-ago software and system security updates were distributed on disks and were manually installed. Today these updates are delivered via the internet and generally require very little user intervention. In many cases no software or security updates are required by you or your team as the service is delivered and managed in the cloud. What is worth noting is, although this has been a very big change, it seemed to occur relatively by stealth and in some ways the change went unnoticed. This is not the case with the Pandemic that has recently occurred. Could you have imagined at the end of 2019, a scenario where there was no travel and all business interactions were done from your living room within three months?

Not only has COVID-19 changed the world – and in particular, business operations – it has significantly increased the attack vector via which a hacker can now access your critical information. Hacks against users working from home have increased to an alarming rate. There has been a surge of two thousand percent in phishing attacks since the virus has occurred. Ease of use and access has taken precedence over security and how companies are storing and sharing critical information is often bypassing any protections that were in place prior to the pandemic. In the battle between security and business continuity, security is often the loser. In addition, many home users have very little security associated to their home systems and we are creating the perfect opportunity for hackers.

Unfortunately, security follows change and it is often playing catchup. A great example of this is the well documented security issues faced by unified communications company Zoom when the recent pandemic thrust them into the spotlight overnight. Sometimes organisations can go through these complications and recover, other times it is these complications that can bring a company to its knees.

It is because of all this change that we must look at technologies that allow us to adapt and move faster. We must look for technologies that can find needles hidden within haystacks. By 2025 we are expected to reach 175 Zettabytes of data worldwide with more than 50% of this data being stored in the cloud and 80% of this data being unstructured. We cannot secure this information without the use of machine learning which processes information in minutes rather than hours, which is often the case with human analysis.

AI like machine learning can assist security analysts when responding to threats and can allow systems to automate responses.

How Does AI Work In IT Security?

01

Learning

Being able to consume terabytes of structured and unstructured data gained from multiple sources and compare this data quickly, using machine learning techniques, AI is continually improving the ability to learn potential security threats and cyber risks more quickly and efficiently.

02

Reasoning

AI can then identify the relationships between threats, for example; malicious files, suspicious IP addresses, geo location information etc. and can very quickly pull all data together to provide better visibility on the potential threat and a more detailed picture on related activity.

03

Augmenting

AI eliminates time-consuming research tasks and provides a curated analysis of risks. This significantly reduces noise and the amount of time a security analyst can take to make a critical decision. In many situations systems can be configured to orchestrate automated responses to remediate the threat with no user intervention.

With AI, rather than running through a list of instructions like a procedural programming language, AI methods maintain a database of instructions and acts on the data as a variable. The selection of the next action to take relies on the application of probabilities.

As computers don't suffer the issues that humans are subject to, such as tiredness and distraction, AI will often discover relationships that may go unnoticed by an analyst. Another advantage of using AI is that computers don't sleep – nor do they take holidays or get sick – so the monitoring of your network and associated systems is continual and in real time. This is important as hacks often occur while you sleep.

Many of the Vendors we partner with are now building AI intelligence into their product offerings. Often this is an additional function available to you within the licensing that you have already purchased. Understanding the advantages that implementing AI can potentially provide you may be the difference from becoming a victim or stopping the threat before it happens. By understanding what normal behavioural activity is and what seem to be deviations from this normal activity, potential threats can be highlighted and dealt with faster.

A simple example of how this works can be case where a user normally accesses the network between the hours of 9am and 5pm and from the same location. This user normally accesses files associated with the marketing department. If that behaviour changes – for example, perhaps the user has now accessed the network from an international location, or at an odd hour, or perhaps even accessed the wrong type of files. AI can detect and identify this abnormal behaviour faster.

Will AI take our Jobs?

AI is not designed to replace the Analyst or human interaction, but it is designed to reduce the noise and simplify the decision-making process by collating data from multiple sources and providing the analyst with more accurate and comprehensive data in a much shorter time frame, enabling the analyst to make a determination faster and potentially avoid an issue, or if not, minimise the impact.

Another potential use for AI is the collection and comparison of data obtained from several geographical locations. With the help of simple smartphone applications, people can give real-time feedback about the conditions in their surroundings – such as traffic congestion. It could also be used to gather information for marketing activity, or to provide hazard alerts. For example, in a smart city environment, being able to predict an area of the city where congestion is occurring and re-route people away from this congestion can be advantageous. By understanding the severity of a problem in real time, users can devise ways of addressing the issue faster and minimise the impact – which is the desired outcome if any issue.

AI is also the perfect partner for the use of automation. For example, where AI has determined a potential breach may be occurring on the network, there is the option having this trigger an automated response as can be seen with many Vendor products – such as a configuration of the firewall to stop certain traffic from leaving the network, or the isolation of an infected endpoint from the network to prevent further issues until the event can be investigated further.

Therefore, the answer to the question is yes, AI is here to stay, and it is already changing the way we do almost everything. As new technologies are developed, and vendors continue to integrate AI into their offerings we will continue to see significant changes in the way we approach not only IT security, but so many of our day to day activities.

seccomglobal.
The Cyber Security Company

WWW.SECCOMGLOBAL.COM

1300 FIREWALL