The Role of Artificial Intelligence in Cybersecurity

Written for KAMIND, IT, Inc.

By Ravi Das

Introduction

As we start to wind down 2019, and venture onwards into 2020, there is one thing that will be certain for Corporate America: Cyberthreats and their attackers will abound, but the difference this time will be that they will be stealthier and more covert in what they do.

In other words, gone are the days of the so called "Smash and Grab" campaigns, where the goal of the Cyberattacker was to launch an all-out, brute force attack against a target and harvest whatever they could.

But now, the Cyberattacker is very deliberate and calculative in every move that they make. For example, they take their own time to deliberately study the profiles of their intended victims, and once the appropriate weak spot has been found, they make their move.

But the goal is not to stay in for just short periods of time; but rather for long ones, in an effort to steal as much as they can, in small amounts, so that the victim will not realize what is going on until it is way too late.

In fact, many Cyberattacks like these often go unnoticed, evading all means of defensive protection that have been deployed by the business. So, is there a way that these threat vectors can get noticed and get mitigated in time before further damage is caused?

Yes, there is. The answer comes through the use of Artificial Intelligence (AI) tools. This kind of technology can virtually learn and detect just about any looming threat and alert the IT security staff so that proper re-mediative actions can be taken.

This is the goal of this whitepaper. It is important to keep in mind that artificial intelligence is still an emerging concept from within Cybersecurity and is very broad in nature. Thus, the primary goal is to provide a general overview of this exciting technology.

What Is Artificial Intelligence?

When one thinks of the term "Artificial Intelligence", very often, an image of the human brain is conjured up. To a large extent, this is a good graphical representation of what it is. The basic idea of this is to mimic the thought and behavioral process of the human brain, to learn, and to apply these "experiences" towards discovering hidden trends and predicting the future. Specifically, artificial intelligence can be defined as follows:

"The term artificial intelligence (AI) refers to computing systems that perform tasks normally considered within the realm of human decision making. These software-driven systems and intelligent agents incorporate advanced data analytics and Big Data applications. AI systems leverage this knowledge repository to make decisions and take actions that approximate cognitive functions, including learning and problem solving."

Artificial intelligence (AI) also makes it possible for machines to learn from experience, adjust to new inputs and perform human-like tasks."

(SOURCE: 1 and 2).

As one can see from the above definition, the potential that Artificial Intelligence has in Cybersecurity is quite enormous. For example, many IT security teams of today use many kinds of tools from various kinds of vendors in order to beef up their lines of defenses.

As a result, they are completely inundated and flooded with all sorts of information and data coming in from all sources. Because of this, there are many false positive warnings and messages that are created, thus putting a huge, extra burden for the IT security team to filter through.

But with the use of an Artificial Intelligence, it can use the concepts of data warehousing in order to instantaneously filter through all of this and provide warnings and messages that are truly indicative of an impending threat vector. In this regard, Artificial Intelligence has also started to make its splash as a task automation tool for both Penetration Testing and Threat Hunting Teams.

As a result, these teams can now devote more time and attention to unearthing all unknown gaps and vulnerabilities that are in existence from within an IT Infrastructure and providing timely solutions for the client on the re-mediative actions that they need to take.

Another area where Artificial Intelligence is in the area of staff augmentation. At the present time, there is a severe worker shortage in the Cybersecurity Industry, as there are currently some 3.5 million jobs that still remain unfilled.

(SOURCE: 3).

In this regard, tools can be used to help predict what the future Cyber Threat Landscape will look like, and even provide recommendations to the IT Security Staff as to how best prepare for it. Typically, this would be the role for the Cybersecurity Analyst, but until enough positions are filled in this aspect, Artificial Intelligence will literally become the "virtual" version of it.

The Sub Fields of Artificial Intelligence

Believe it or not, the field of Artificial Intelligence is actually a derivative of other fields, namely the following:

- Philosophy;
- Logics and Mathematics;
- Computational Algorithms;
- Psychology and the Cognitive Sciences;
- Neurosciences;
- Evolution.

Out of this above list, it is the second through the fifth that are deemed to have the most importance and relevance to Artificial Intelligence. For example, it is the logical structure of the mathematical algorithms that are used to "learn" from previous examples and apply those rules in making decisions for future decisions; in terms of Psychology, the principles of how the mind and brain interact with each other is also applied; and finally, in regard to the Neurosciences, Artificial Intelligence tools also try to imitate, or mimic, the neuronic activity of the brain, especially in the way that neurons either fire or do not fire.

In fact, Artificial Intelligence (AI) can be further subdivided into two main types of classification, which are as follows:

1) Type 1:

   This consists of the following:

   - Weak, or "Narrow" based Artificial Intelligence:

     In this scenario, the AI system is focused on just accomplishing one specific task or goal. This can be considered to be a very primitive form of it, as it can only do very basic tasks, such as playing against a competitor in a basic Chess game. In this situation, all the rules and probable scenarios must be fed manually into the AI system before it can engage a true competitor. In other words, it cannot learn on its own, each and every time that a new game is played, all the rules and outcomes have to be fed into it each and every time.

   - Strong Artificial Intelligence:

     This is the kind of AI that is used most typically in Cybersecurity today. For example, based upon the data and intelligence feeds that are fed into it, this kind of system can literally learn all on its own from past observations, and use that knowledge in order to make informative decisions for the future. In other words, every effort is made so that it can emulate the human thought and decision-making process as much as possible. The key differentiator here is that there is almost no human intervention needed for these kinds of AI systems; the only time this is really ever needed is if new information and data feeds have to be inserted.

2) Type 2:

   These kinds of Artificial Intelligence systems are based upon the functionalities that they possess or are anticipated to in the future. These include the following:

   - Reactive Machines:

     This is considered to be the most rudimentary, or basic form of an AI system, and in fact is more like a Type 1, as just reviewed. In particular, their memory is very limited, and these kinds of systems can only store very limited amounts of information and data and cannot make future decisions or predictions on their own, without some sort of human intervention.

   - Limited Memory:

     These are the Artificial Intelligence systems that can "learn" from past examples and use those to make decisions for future events. In fact, this is the classification that is more representative of AI systems that are in existence today, and that are used in the Cybersecurity Industry today.

   - The Theory of the Mind:

The main purpose of this kind of Artificial Intelligence system is to "... emotion, belief, thoughts, expectations and be able to interact socially."

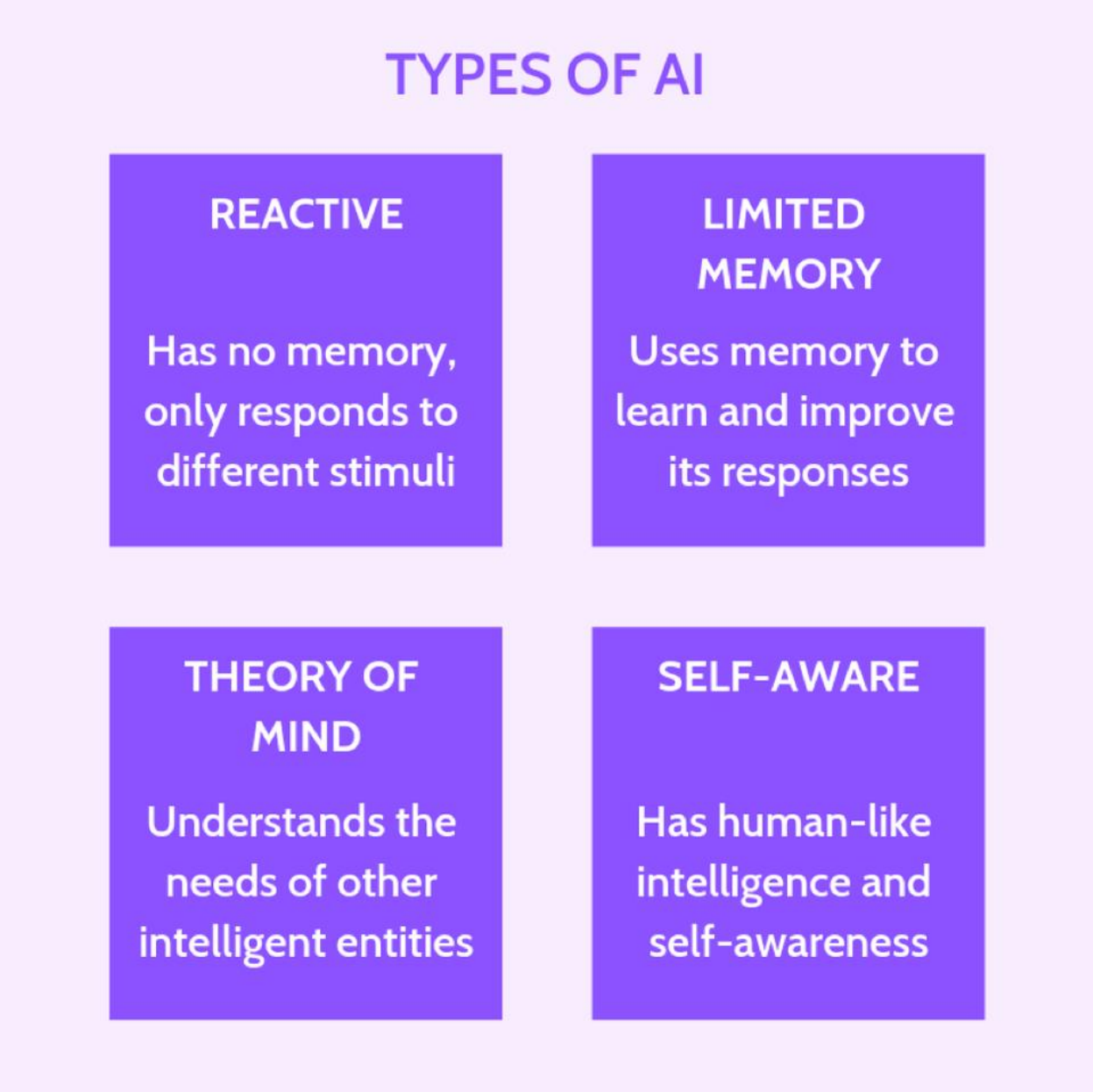
(SOURCE: 4).

Although this has a very long way to go until it can even come remotely close to achieving the above, we are already seeing some very basic forms of this starting to take place. The best examples of this are the Virtual Personal Assistants, namely those of Alexa, Siri, and Cortana. These kinds of applications try to learn our thought and decision-making profile so that recommendations and directions can be provided based upon previous actions.

- Self-Awareness:

  This would be the ultimate goal of any Artificial Intelligence system. This entity would be very much like a being and even act like one. The best, illustrative example of this is the character Data from the TV series, "Star Trek: The Next Generation".

These two classifications are illustrated below:



(SOURCE: 4).

There are also many subspecialties from within Artificial Intelligence, and these are as follows:

1) Data Science:

   As mentioned, the Cybersecurity Industry at the present time, and going well into the foreseeable future, is experiencing a huge influx of information and data. It can take an entire IT Security staff literally days or even weeks in order to comb through all of this. Of course, we all know that this simply an almost impossible task to be achieved. In this aspect, Artificial Intelligence can be viewed as the ultimate "Savior" when it comes to analyzing these huge datasets, also known as "Big Data". Within just a matter of seconds, hard to detect and unseen

trends can be noticed very quickly, and recommendations can be even be provided as to how they should be applied when modeling the Cyber Threat Landscape.

2) Machine Learning (ML):

This subspecialty can be considered as an extension of the above, but with the main difference being that super sophisticated mathematical algorithms are used to help the IT Security team to classify, put into specific categories, and even predict data extrapolations from any given dataset. These mathematical algorithms are actually coded into a specific programing language (such as that of Python, as an example) in order to help create and build an entire Machine Learning system. This is the one area of Artificial Intelligence that can be used to help filter through false positives and determine those which are for real or have some merit to them to warrant further action.

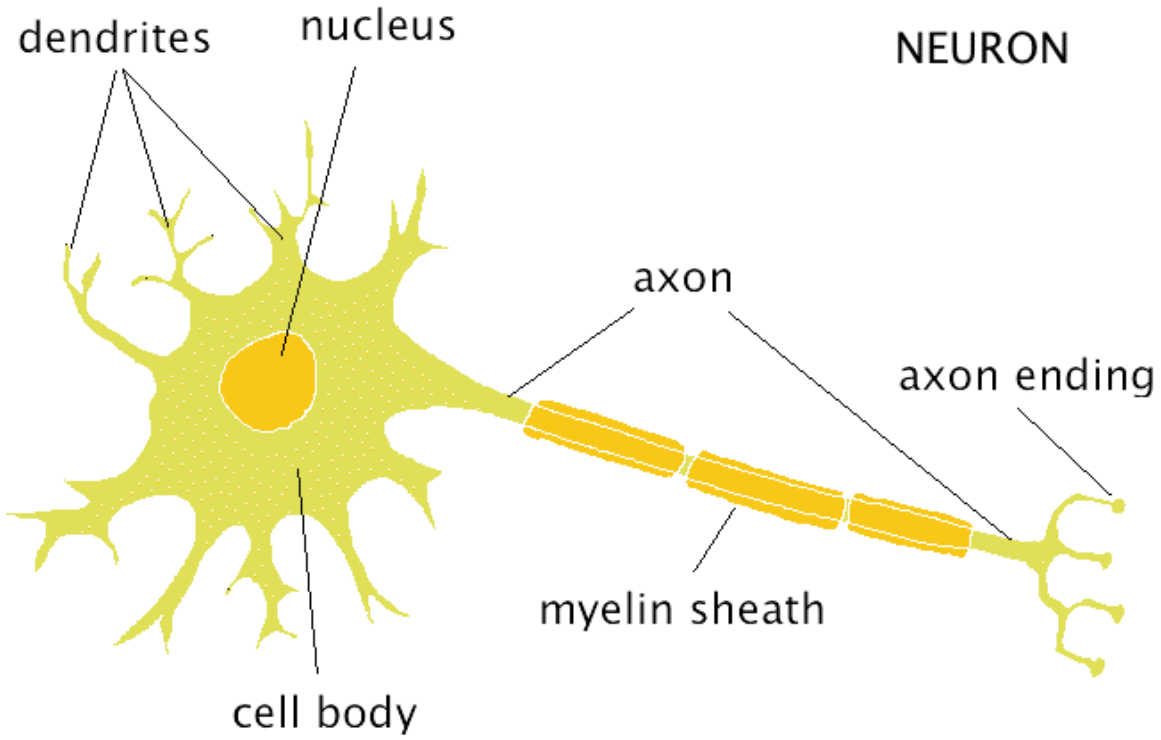
3) Neural Networks (NN):

This is the area of Artificial Intelligence that tries to mimic the Central Nervous System and the Neurological functions of the human brain. It is the Neuron that forms the basis of these two, and it can be defined specifically as follows:

"The neuron is the basic working unit of the brain, a specialized cell designed to transmit information to other nerve cells, muscle, or gland cells. Neurons are cells within the nervous system that transmit information to other nerve cells, muscle, or gland cells. Most neurons have a cell body, an axon, and dendrites."

(SOURCE: 5).

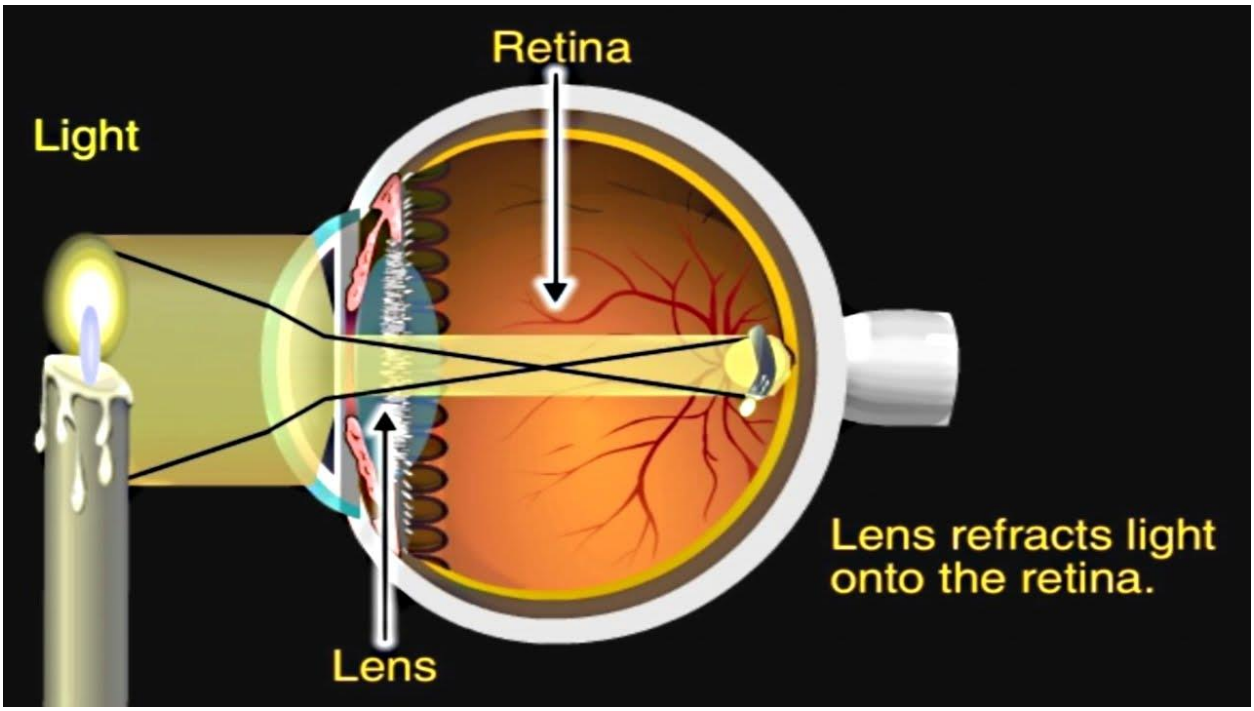
In fact, it is estimated that the human brain has an average from 100 million to 100 billion neurons, all connected amongst one another. The primary goal of a Neural Network system is to map these interactions, and hard code them so that they can be used for predictive behaviors, such as modeling the Cyber Threat Landscape. A typical neuron is illustrated below:



(SOURCE: 6).

4) Image Processing:

Without a doubt, every waking moment of our lives is spent in seeing objects on a daily basis. This information is of course captured by the eye and then transmitted to the brain via the Optic Nerve (which is the collection of blood vessels at the back of the eye) so that vision becomes possible. This is illustrated below:



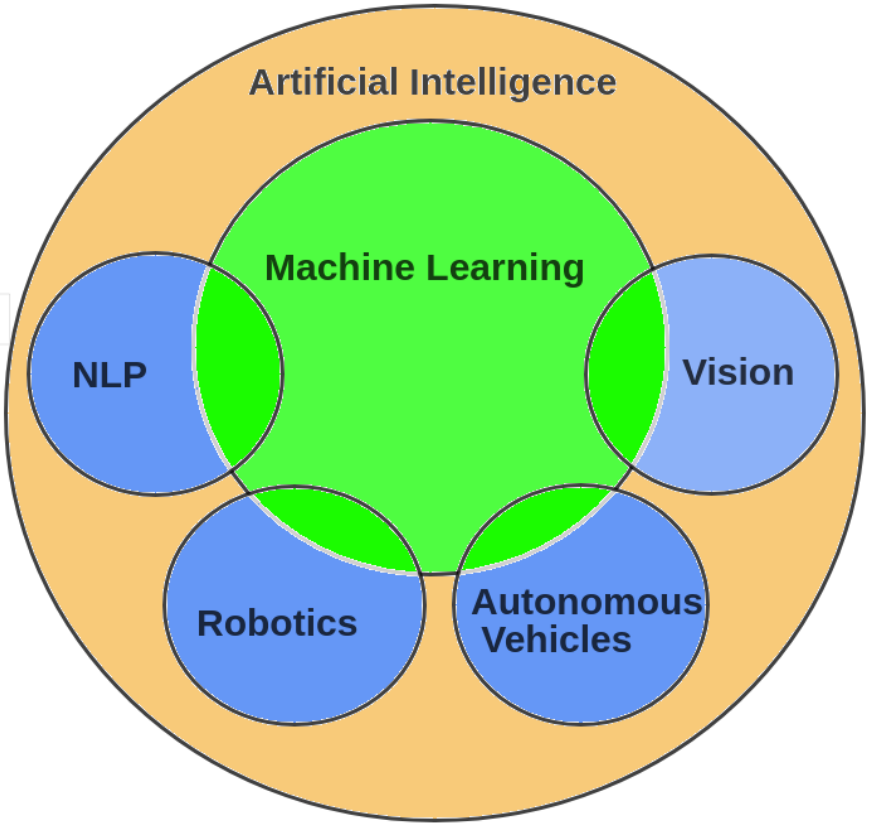
(SOURCE: 7).

This is the area of Artificial Intelligence that attempts to mimic this entire process. This is also very often referred to as "Computer Vision". One of the best examples of where this application is being used at is in Facial Recognition. This is a Biometric Technology that is very often used in conjunction with CCTV Technology, in order to confirm the identity of a particular individual. But by incorporating Computer Vision into these two, the robustness and reliability of a 100% identification system is made that much more possible.

5) Robotics and Embedded Systems:

Simply put, this is where Artificial Intelligence tools are being created and deployed into robots. This kind of technology is most widely used in the manufacturing industry, where they can perform very mundane and routine tasks on an automated basis with a much higher level of accuracy, and of course, at faster speeds as well.

These subspecialties of Artificial Intelligence are illustrated in the diagram below:



(SOURCE: 8).

The Role Of Artificial Intelligence In Cybersecurity

An Overview of the Applications of Artificial Intelligence In Cybersecurity

Artificial Intelligence can be used in the Cybersecurity Industry in many ways, which are still yet to be tapped into. Just as much as other technologies are constantly and dynamically changing, so too is this field. It has just started to make its debut for security applications, and there is a long way to go yet until it is fully adopted and deployed. But Artificial Intelligence is being used in some key areas in Cybersecurity, which are as follows:

- Many Cyberattacks are starting to go unnoticed today. There are two primary reasons for this:

  1) The IT Security team is so overworked that they are simply, through no fault of their own, are letting the real threat warnings and alerts fall through the cracks;
  2) The Cyberattacker is becoming so sophisticated that many of the threat vectors that they do launch are very often not detected by the security tools that have been deployed at the lines of defenses.

  Through the use of Artificial Intelligence tools, many of these kinds of attacks are now starting to get noticed, and by establishing a threshold of interoperability with other devices (such as Network Intrusion Devices, Firewalls, Routers, etc.) these kinds of threat vectors are now getting

stopped in their tracks even before they make an entry into the IT and Network Infrastructure of an organization.

- As it has been described previously, the severe shortage of skilled workers in the Cybersecurity Industry has left a huge void that needs to be filled by the existing employees in the workplace. Thus, this is adding on an even extra layer of burden and workload, especially when it comes to conducting routine and daily tasks. In this aspect, Artificial Intelligence can automate these kinds of job functions, thus allowing the IT Security staff to focus in on the more crucial areas of their job functions. Another added benefit is that depending upon the tool that is being used, many Artificial Intelligence systems of today do not require any sort of human intervention. This simply means that once they have been programmed to any certain kinds of tasks, the reliability of them to deliver a high-quality product is quite robust. The graphic below clearly demonstrates how the use of Artificial Intelligence can help augment an IT Security staff, based upon the number of labor hours that can be saved by automating the following tasks:

Table 1. Labor hours spent containing cyber exploits each week	Not facilitated by AI	Facilitated by AI	Difference in hours and cost
Organizing and planning approaches to cyber defense	25.32	16.05	9.27
Capturing actionable intelligence about cyber exploits and malware infections	80.20	41.11	39.09
Investigating and detecting application vulnerabilities	195.88	70.48	125.40
Investigating actionable intelligence about cyber exploits or malware	66.28	24.23	42.05
Cleaning, fixing and/or patching networks, applications and devices (i.e., endpoints) damaged/infected by cyber exploits or malware	212.89	39.63	173.26
Documenting and/or reporting upon the cyber event (in conformance with policies or compliance mandates)	25.07	15.91	9.16
Time wasted by security staff members chasing erroneous or false positives	400.83	41.42	359.41
Unplanned downtime due to cleaning, fixing or patching of malware-infected networks, applications and devices	3.95	1.90	2.05
Total hours per week	1,010.42	250.73	759.69
Total hours per year	52,541.84	13,037.96	39,503.88
Estimated total cost per year	$3,283,865.00*	$814,872.50*	$2,468,992.50*

*IT and IT security fully loaded pay rate is $62.50 (source: Ponemon Institute).

(SOURCE: 12).

- In Cybersecurity today, one of the hot topics that is coming about is that of Multi Factor Authentication, or “MFA” for short. This is where more than one layer of defense is used in order to protect IT and Network Assets. For example, rather than just a using a password to gain access to shared resources, there are other authentication mechanisms that an individual will have to go through in order to positively confirm their identity. This could include incorporating the usage of Challenge/Response Questions, RSA Tokens, Smart Cards, Biometrics,

etc. While all of these are very reliable means of authentication when they are used in conjunction with another, there is still fear that a Cyberattacker can still break through any of these. Thus, there is very serious consideration being given to using Artificial Intelligence as yet another layer of authentication. But the difference here is that these kinds of systems can actually build a profile of the end user and allow for authentication based upon that person's predictive behavior. In other words, Artificial Intelligence can make a holistic judgement (based upon an infinite number of variables) in real time if the end user is really claiming with 100% authenticity whom they are to be.

- At the present time, Artificial Intelligence is being used to aid in the protection of certain aspects of the IT and Network Infrastructure, from both a hardware and software application standpoint. In other words, it is only being used in local instances, not at an enterprise level, which will encompass the entire organization. It is highly anticipated, by the way that the AI technology is rapidly advancing, that this particular level of protection will become a reality in the short term.

- One of the oldest and still most widely used form of threat vectors that is used is that of Phishing. There are many new variants of it that are coming out today, especially in the way of Business Email Compromise (also known as "BEC") and Ransomware. Once again, there are so many of these that are rampant today that it is close to impossible for an IT Security staff to keep up with all of this. For example, it has been cited that 1 out of every 99 Email messages is a Phishing based one. While that may not seem like a lot, just think about the total number of messages that are sent in one day from just one business. This ratio can multiply at least 100X. An Artificial Intelligence tool can track these notorious Emails much quicker than any human being can at a rate of 10,000 messages at any given moment in time. Another advantage of using Artificial Intelligence there are no geographic limitations in which it can detect for Phishing Emails (it can virtually understand any language if it has been programmed that way), and it can also differentiate between a spoofed website and an authentic one in just a matter of seconds.

  (SOURCE: 13).

The Functionalities, or Characteristics Of An Artificial Intelligence System In Cybersecurity

As it relates to Cybersecurity, there are three main functionalities of an Artificial Intelligence system which makes it very different from the other security tools that are available. They are as follows:

1) It can learn:

   One of the main themes that has been pointed is that a good AI system can learn, with or without human intervention (of course, the latter is much more preferred). The way that it learns is that literally billions of pieces of data are fed into it, via many intelligence feeds. Once this data is fed into it, the Artificial Intelligence tool can then "learn" from it by unearthing any trends or threat vector-based attack signatures that have not been discovered previously. It can even also learn from known trends as well. By combining these two together, the AI system can then make reasonably accurate observations or predictions as to what the Cyber Threat Landscape will look like on a daily basis, if that it is what the main purpose of has been designed to accomplish. It is important to note, while this is done on a 24 X 7 X 365 basis, the data and

information that is fed into it must be done on an almost minute by minute basis. If this is not done, the AI system can lose its robustness very quickly, can literally become "stale". Also, based upon the datasets that are fed into it, a good AI system can also even make recommendations to the IT Security team as to what the best course of action it can take in just a matter of minutes. In this regard, Artificial Intelligence can also be used as a vehicle for threat mitigation by the Cyber Incident Response Team. An AI system that is designed for the Cybersecurity Industry can also digest, analyze, and learn from both structured and unstructured datasets (this even includes the analysis of written content, such as blogs, news articles, etc.).

2) <u>It can reason</u>:

Unlike the other traditional security technologies, Artificial Intelligence tools can also reason and even make unbiased decisions based upon the information and data that is fed into it. For example, with very high levels of accuracy and reliability, it can "... identify the relationships between threats, such as malicious files, suspicious IP addresses or insiders." (SOURCE: 9). In other words, an AI system can look at multiple threat vectors all at once and take notice of any correlations that may exist between them. From this, a profile of the Cyberattacker can be created and even used to prevent other new threat variants from penetrating into the lines of defenses. Very often, a Cyberattacker will launch differing attacks so that they can evade detection. For example, Cyberattackers have been known to hide their tracks after penetrating an IT/Network Infrastructure by covertly editing the system logs of the servers, or even just simply reset the modification date on a file that has been hijacked but replaced with a phony file. These cannot be detected by the standard Intrusion Detection Systems (IDSs) that are being used today; they can only be discovered by anomalies if significant deviations can be found. But with the use of AI, these and other hidden commonalities can be discovered very quickly in order to track down the very elusive Cyberattacker. Also, an AI system does not take a "Garbage In/Garbage Out" view of a threat vector. It tries to make logical hypotheses based upon what it has learned in the past. In fact, it has been claimed that Artificial Intelligence can respond to a new threat variant 60X faster than a human could ever possibly do.

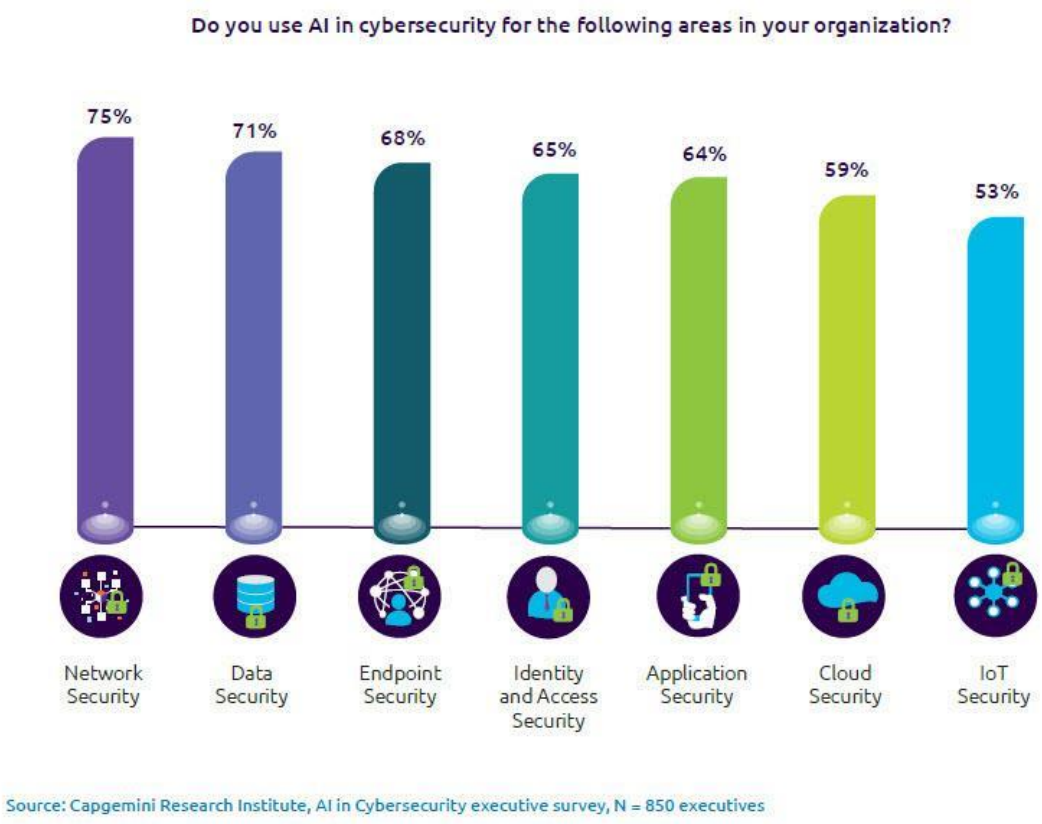
(SOURCE: 9).

3) <u>It can augment</u>:

Again, as it has been mentioned before in the last subsection, one of the biggest advantages of Artificial Intelligence in Cybersecurity is that it can augment existing resources. Whether it is from filling the void from the lack of the labor shortage, or simply automating routine tasks that need to be done, or even filtering through all the false positive warnings and messages to determine which of those are for real, AI can absorb all of these time consuming functions that can take an IT Security team hours to accomplish and get them done in just a matter of minutes. It can also be a great tool to conduct tedious research-based tasks, can calculate the levels of risk very quickly so that the IT Security team can respond to a Cyber Threat in just a matter of seconds and mitigate it quickly.

To further substantiate the need for Artificial Intelligence in Cybersecurity, a recent study by Capgemini (which is entitled "Reinventing Cybersecurity With Artificial Intelligence") discovered the following:

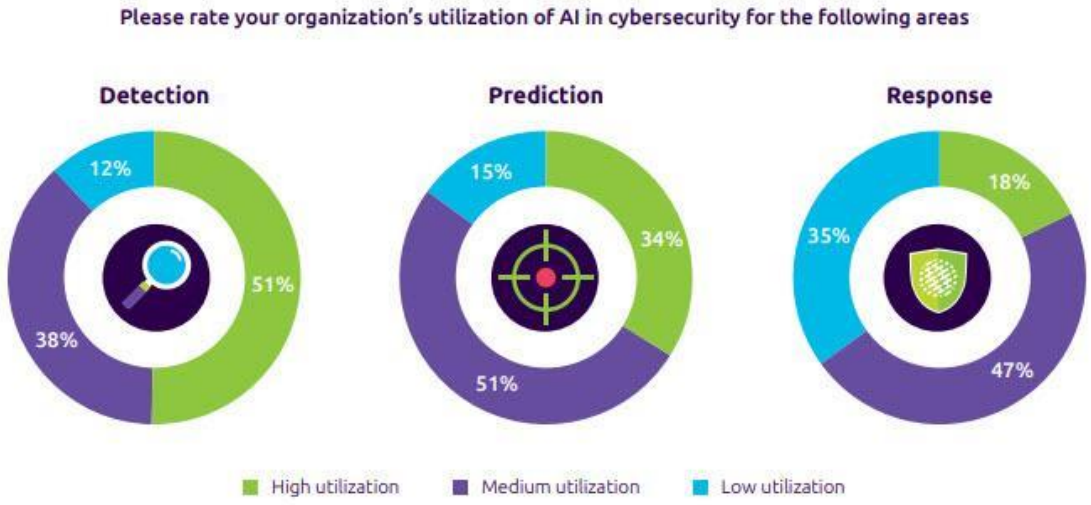
- 64% of businesses feel that they need robust AI tools in order to combat the threat from Cyberattackers;
- 73% of businesses are now developing test cases for using Artificial Intelligence primarily for Network Security purposes. This is illustrated in the diagram below:



(SOURCE: 10).

- 51% of CIOs and CISOs are planning to make extensive use of Artificial Intelligence as it relates to Threat Hunting and Detection. This is illustrated below:

Figure 3: Higher utilization of AI for detection than prediction or response



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

(SOURCE: 10).

- 64% of the CIOs and CISOs claim that using Artificial Intelligence actually decreases the time it takes to respond to a particular Cyberattack, and the corresponding response time has increased by 12% as can be seen in the diagram below:

Figure 4: AI in cybersecurity lowers the cost to detect and respond to breaches

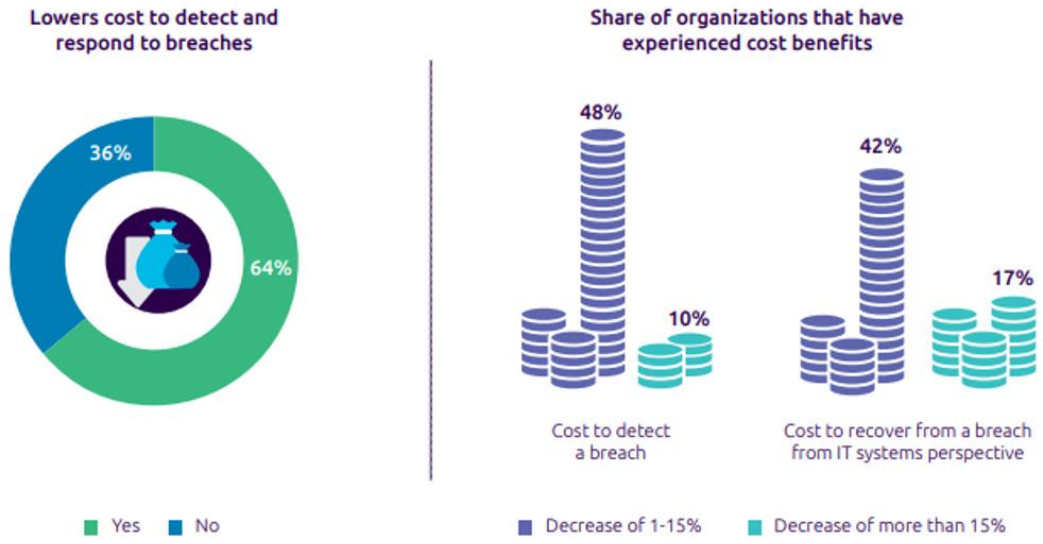
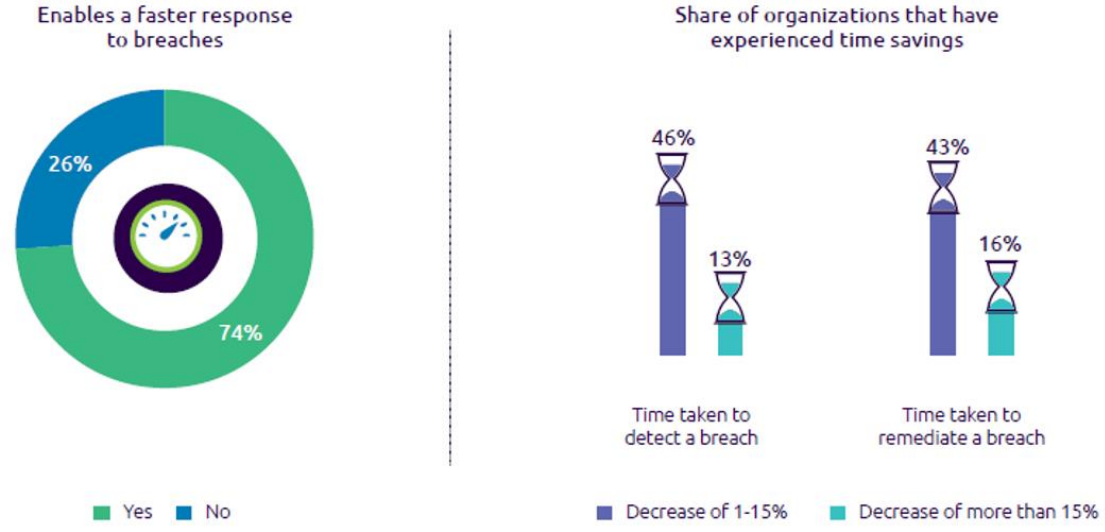


Figure 5: Nearly three in four executives say AI in cybersecurity enables a faster response to breaches



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

(SOURCE: 10).

- The top 5 use cases for Artificial Intelligence are as follows:

  *Fraud Detection;

*Malware Detection;

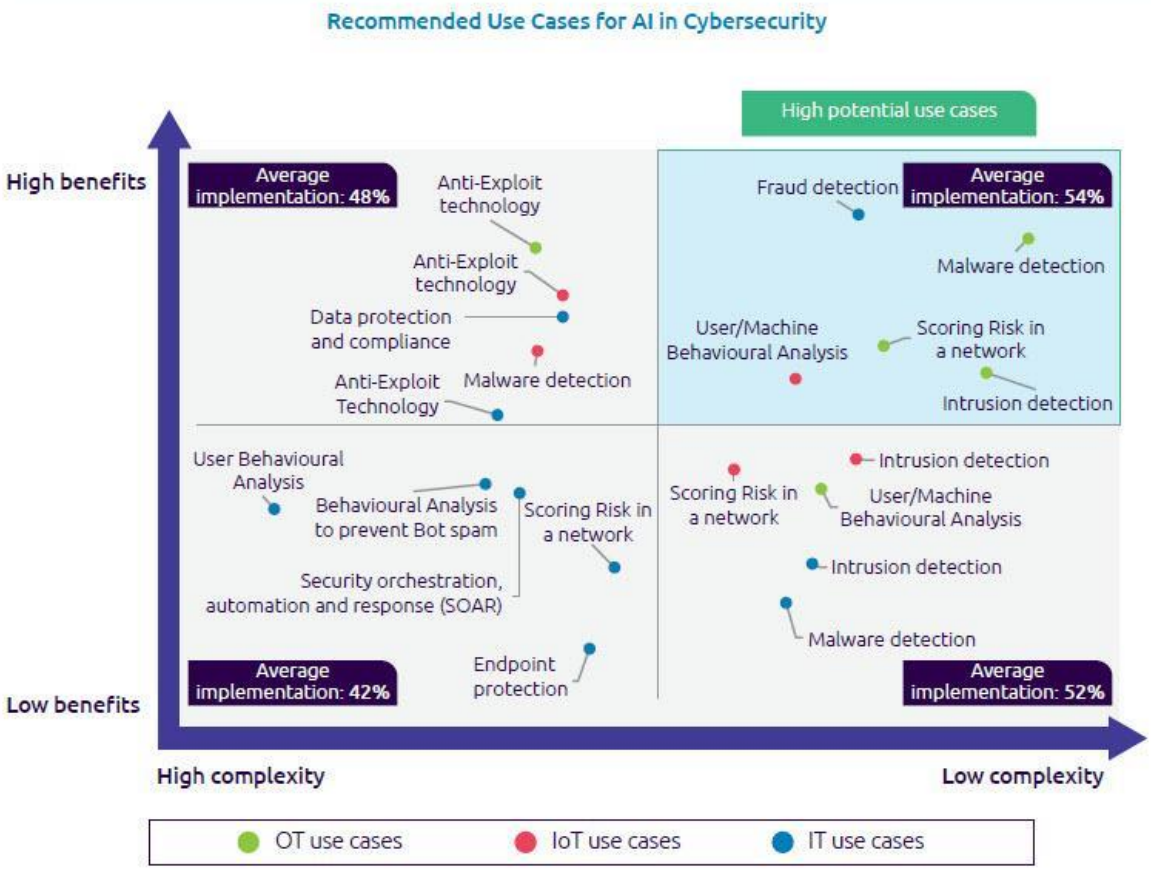
*Intrusion Detection;

*Calculating risk levels for Network Security purposes;

*Behavioral Analyzes.

This can be seen pictorially below:

Figure 7: OT and IoT use cases have higher rates of adoption



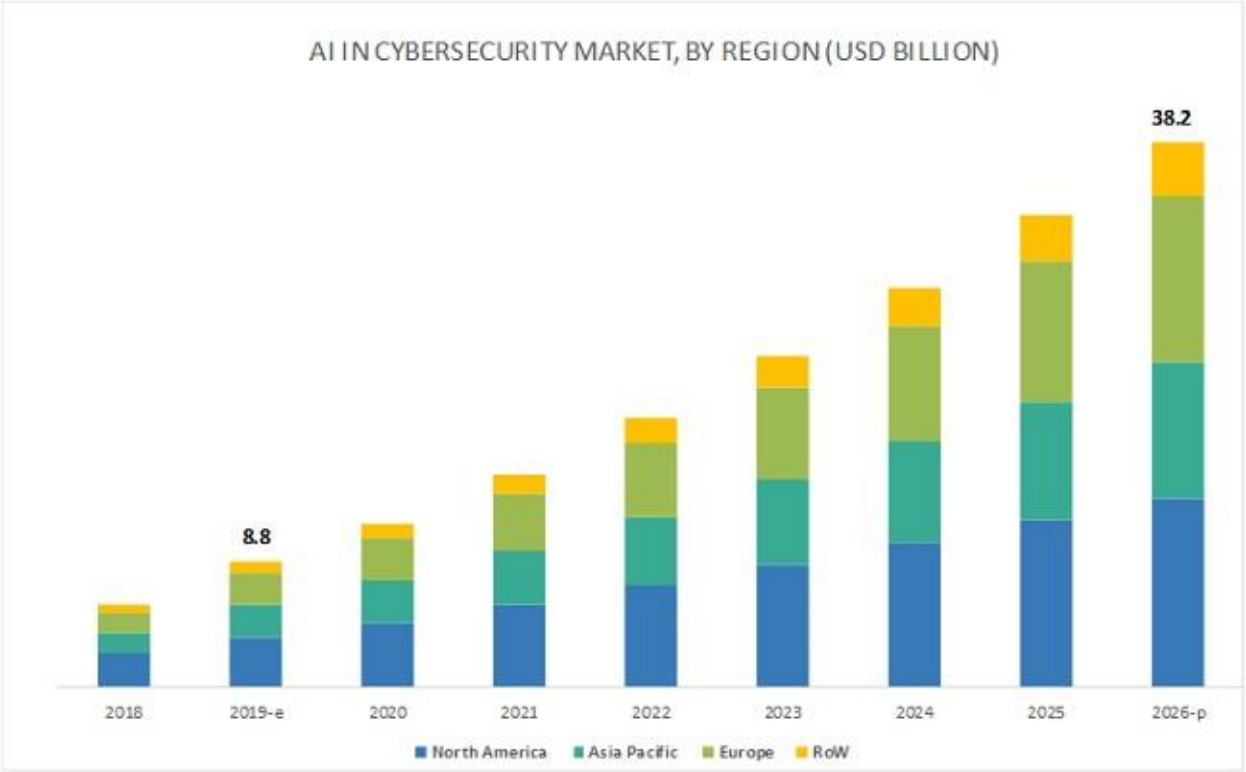
Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives
Average implementation: Share of organizations that have deployed the use cases in quadrant at first level, multiple, or full-scale deployment.

(SOURCE: 10).

- An overwhelming 56% of Cybersecurity Executives claim that their respective staffs are too overworked and overburdened; and that an alarming 23% of these teams cannot even respond to Cyber threats as they occur;
- 48% of the CIOs and CISOs claim that plan to increase their budget for Cybersecurity by at least 29% in 2020.

It is important to note that 850 CIOs and CISOs as well other security executives were polled in this survey. Further details on this study by Capgemini can be seen here at this link.

Overall, it appears that the spending on Artificial Intelligence in the Cybersecurity Industry will grow exponentially in the coming years, as substantiated by the diagram below:



(SOURCE: 11).

Overall, it is expected that in the United States, the spending on Artificial Intelligence technologies will be at $38.2 billion by 2026. The main catalysts for this growth are as follows:

- The rise of interconnected devices brought on by the evolution of the Internet of Things (IoT);
- The overall growth rate of newer Cyber Threat variants;
- Concerns of information and data leakage;
- The increasing vulnerability of Wi-Fi networks;
- The security posed by the various Social Media platforms (which include the likes of Facebook, Twitter, Linked In, Instagram, Pinterest, etc.);
- The need for secure cloud services by the Small to Medium sized Business (SMB) market.

(SOURCE: 11).

Conclusions–How To Your Business Ready For Using Artificial Intelligence In Cybersecurity

Overall, this whitepaper has examined what Artificial Intelligence actually is, is components, as well as its relevance and importance to Cybersecurity. You may be thinking now, after reviewing the benefits of what Artificial Intelligence can bring to the table, that you are ready to deploy it in your business. But keep in mind that this is no easy task, as you are adding in a totally new system that should operate

seamlessly with your other security related functions and processes. How you actually implement an AI system at your business will depend completely upon what the security requirements are, and the assets that currently exist in your IT and Network Infrastructure. You should work closely with the vendor from whom you are procuring your AI system from in order to work out an finalize all of these details.

But the following is a general checklist that will prove useful in your consideration of the deployment of an Artificial Intelligence system:

1) <u>You must find the right kind of data sources to be used</u>:

   The bottom line is that an Artificial Intelligence system is only as good as the datasets that are fed into it for learning purposes. Therefore, very careful consideration needs to be given to the selection of those datasets that you plan to use. For example, they must not only be relevant to the tasks that you are trying to accomplish with your AI system, but they must be the most up to date. In this instance, give serious consideration to using the "SOAR" Model. Essentially, it is an acronym that stands for the following:

   ***<u>S</u>**ecurity **<u>O</u>**rchestration

   ***<u>A</u>**utomation

   ***<u>R</u>**esponse

With Security Orchestration, you and your IT Security staff are bringing together all the available datasets that you are planning to make use of and making them all work together as one, cohesive unit. Some features of Security Orchestration include the following:

- Having a standard set of AI dataset collection processes;
- Providing a single platform in which the Artificial Intelligence system can compile and retrieve information and data as they are collected in real time;
- Providing a unified dashboard from which all ***<u>legitimate alerts and warnings</u>*** can be further examined.

2) <u>Select the right platform</u>:

   Once you have selected the datasets that you intend to use with your Artificial Intelligence system, the next step then is to design the platform from which this they be leveraged into it. In other words, this is the feed that will pump these datasets in. Equally important is to implement some sort of automated Quality Control (QC) check processes to ensure that the datasets are not only current, but that they are also accurate and secure as they are being fed into the AI system.

3) <u>Conduct pilot tests of how it all operates</u>:

   As with any new security technology, you must first confirm that the Artificial Intelligence system will actually operate and perform to its expected levels. This should be done in a controlled, or a "sandbox" environment first. To do this, start with those use cases that are most relevant to your security requirements. In order to confirm that your AI system is starting

to learn both effectively and efficiently, start with the simpler ones first that have the most current data. Then use this in which to launch more complex use cases and datasets to make sure that the AI system is operating to its expected levels. Once all objectives have been met in this controlled environment, then it should be rolled out into production, where it will work and commingled with the other security tools that are deployed in your business. But this is a process that must be conducted on a regular basis, in order to ensure that the Artificial Intelligence system is not going "stale", and still remains in an optimal and robust state, as described previously.

4) Establish a governance program:

After the Artificial Intelligence, you also need to deploy some sort of strategy, or "game-plan" that will set forth the framework in which your IT Security staff can make sure that the AI system is continually learning, and is delivering on its expected outcomes, based upon the Key Performance Indicators (KPIs) and other metrics that have been set forth. In fact, this is an absolutely crucial stage, because you are relying upon it on a daily basis in order to combat and mitigate any existing and potential Cyber Threat variants.

Sources

1) https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html
2) https://www.datamation.com/artificial-intelligence/what-is-artificial-intelligence.html
3) https://cybersecurityventures.com/jobs/
4) https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/#301ec3a6233e
5) https://www.brainfacts.org/brain-anatomy-and-function/anatomy/2012/the-neuron
6) http://webspace.ship.edu/cgboer/theneuron.html
7) https://www.youtube.com/watch?v=YcedXDN6a88
8) https://medium.com/@chethankumargn/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b
9) https://www.ibm.com/security/artificial-intelligence
10) https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/#187aab24117e
11) https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-security-market-220634996.html
12) https://www.plugandplaytechcenter.com/resources/how-artificial-intelligence-transforming-cybersecurity/
13) https://www.entrepreneur.com/article/339509
14) https://www.cs.bham.ac.uk/~jxb/IAI/w2.pdf
15) http://technoitworld.com/5-artificial-intelligence-fields-changing-way-things-work/
16) https://aboutssl.org/role-of-artificial-intelligence-in-cyber-security/
17) https://www.cncs.gov.pt/content/files/cybersecurity_and_the_role_of_artificial_intelligence-_arlindo_oliveira.pdf
18) http://techgenix.com/cybersecurity-ai/