FROM THE BRAIN TO AI

The brain – a mere 3 pounds/1.4 kilos - is the result of eons of evolution, delivering the ability to analyze complex situations and data within less than 150 milliseconds. The processing infrastructure of the brain, the neural network, consists of at least a hundred billion neurons receiving, processing, and transmitting information via electrical and chemical signals to other neurons via synapse pathways.

Humankind has spent millennia trying to replicate that processing power. In the 1950s, exploration of AI began using the most primitive computers, taking up full rooms with their machinery and thousands of vacuum tubes.

3000 BCE
The first abacus was recorded to have been used in Ancient Mesopotamia between 2700-2300 BCE.

1997
On May 11, 1997, IBM's Deep Blue, one of the first artificial intelligence-based computers, beat Garry Kasparov in a six-game chess match.

1980's
AI in its most basic form involves mimicking human logic and its way of thinking. It can be as simple as rule-based decision making, decision trees etc. In the 80's a new family of AI algorithms emerged called "Machine Learning".

2010's
Over the course of the decade, deep learning has achieved 20 to 30 percent improvement in most benchmarks of computer vision, speech recognition, and understanding how, outperforming human beings, it’s the greatest leap in performance in the history of AI and computer science.

HUMANKIND HAS SPENT MILLENNIA TRYING TO REPLICATE THAT PROCESSING POWER.

DEEP LEARNING & CYBERSECURITY

"Just as electricity transformed almost everything 100 years ago, today I actually have a hard time thinking of an industry that I don’t think AI will transform in the next several years."
- Andrew Ng (Co-Founder of Google Brain)

These words spoken by Andrew Ng, a world-renowned computer scientist, imply volumes of the potential that AI has in touching every aspect of our increasingly digitized lives. Indeed, AI and its latter incarnations, machine learning and deep learning, are revolutionizing the way we conduct business, shop, educate, socialize, and no less protect ourselves from impending threats.

As more aspects of our lives take place on a digital sphere, it will need to be a major priority to keep that sphere safe and free from attack. This increasing digitalization will not only make cybersecurity more pertinent than ever before, but the cybersecurity tools we use will need to employ the most advanced form of AI to ensure that it’s up to the task.

We are entering an era where defeat and victory will be determined by one’s technological advantage. And considering what’s invested, it’s a challenge that no one can afford to lose.

The terms artificial intelligence and its subcategories of machine learning and deep learning have become ubiquitous in marketing hype. Therefore, it’s essential we understand the differences between all three and the way they can each be...
In the context of cybersecurity, the term "assumed breach" refers to the approach where enterprises assume that they will be attacked and focus on minimizing the damage rather than preventing the attack itself. This approach is driven by the understanding that traditional methods of cybersecurity, such as firewalls and antivirus software, are often inadequate due to the sophistication and complexity of modern threats, including zero-day attacks and file-less malware.

The evolution of malware has led to an increased focus on machine learning approaches, particularly deep learning, due to their ability to handle unstructured data and adapt to new situations. However, these methods also present challenges, including the need for vast amounts of labeled training data and the risk of overfitting.

For example, in the domain of image recognition, a classic challenge is to identify dogs. A machine learning algorithm might be trained to recognize dogs based on specific features like ear shapes, eye size, and nose size. However, if it encounters a cat with similar features, the algorithm may struggle to distinguish between the two, leading to misclassification.

These challenges highlight the importance of developing robust and adaptable machine learning models that can handle the diversity and complexity of modern threats. While traditional approaches may have limitations, they also offer valuable insights that can be leveraged in conjunction with more advanced techniques to enhance overall cybersecurity measures.
Similar to the human brain, the basis for deep learning, which has been increasingly adopted since 2010’s, is the neural network. A deep learning neural network consists of hundreds of thousands of artificially constructed neuron-synapse combinations, like the human brain, this neural network is not linear. All the neurons in each layer are connected directly to all the neurons in the subsequent layers, allowing for simultaneous parallel processing.

The multiplexed neural networks of the human mind analyze not only what someone is saying based on their speech, but also simultaneously (parallel) process the tone of voice, body language, and facial expressions to get the full interpretation of what those words mean. A neural network defines meaning by looking at the whole – parallel processing; sequential processing would simply analyze the words, without getting the complete understanding. Just as humans process data from multiple senses, the neural network processes all the available data that is inputted.

The multilayered neural networks of the human mind analyze not only what someone is saying based on their speech, but also simultaneously (parallel) process the tone of voice, body language, and facial expressions to get the full interpretation of what those words mean.

Deep neural networks create pathways that go directly from raw data to comprehensive insights. Deep learning uses its neural networks and perceptions, to create its non-linear data patterns that it can apply to new data sets, as directed by specialized deep-neural algorithms.

The deep learning algorithms perform decision-making, removing the need to define attributes and enabling analysis of the big picture by using 100 percent of the available data. They look at every single aspect of the data, the file type, the contents, etc.

This combination makes its results consistently more accurate and intuitive. It can tell the difference between a Pomeranian and a Russian Blue due to the massive number of characteristics from the raw data that it processes to reach a decision – like our own neural networks.

**HOW DO HUMANS LEARN?**
- We hold preconceived premises, facts and theories about a given situation
- We anticipate the outcome of the situation
- The result might be different than we expected
- We adjust our expectations to the result in reality change our future prediction based on the newly learn information

**THE HOLISTIC VALUE OF DEEP LEARNING**
Deep neural networks create pathways that go directly from raw data to comprehensive insights. Deep learning uses its neural networks and perceptions, to create its non-linear data patterns that it can apply to new data sets, as directed by specialized deep-neural algorithms.

The deep learning algorithms perform decision-making, removing the need to define attributes and enabling analysis of the big picture by using 100 percent of the available data. They look at every single aspect of the data, the file type, the contents, etc.

This combination makes its results consistently more accurate and intuitive. It can tell the difference between a Pomeranian and a Russian Blue due to the massive number of characteristics from the raw data that it processes to reach a decision – like our own neural networks.

**HOW DO MACHINES LEARN?**
- The data scientist prepares data samples for training.
- The model is trained by feeding it with millions of samples of labeled data.
- Throughout the training process, the brain learns how to instinctively detect and identify data.
- The brain reaches prediction level, where it makes reasonably accurate predictions.
- Confirmations of predictions help to refine the model’s knowledge.

**THE BENEFIT OF APPLYING DEEP LEARNING TO CYBERSECURITY**
- **RAW DATA TRAINING**
  - Capable of training directly from raw data, it is able to detect a new sample with greater levels of accuracy.
- **INDEPENDENT OF HUMAN INTERVENTION**
  - Does not rely on human intervention to perform feature engineering and data manipulation to detect even new and unknown samples.
- **ANALYZE ANY TYPE OF DATA**
  - The input agnostic development of this algorithm means that Deep Learning can handle any and all types of data.
- **NON-LINEAR CORRELATIONS**
  - It can detect complex nonlinear correlations, it can analyze multiple levels of complex data patterns.
- **UNLIMITED TRAINING SAMPLES**
  - Deep learning continually improves as the training data set constantly grows, it is the only method that can scale into hundreds of millions of training samples.

**GETTING TO THE BIG PICTURE**
Deep learning uses raw data, to scan and analyze every aspect of a file or vector. By the nature of this ability to detect patterns from raw data, deep learning can detect malicious anomalies and predict unknown attacks. The algorithm understands and defines by itself what is relevant - or not, allowing it to find complex non-linear correlations, which are hard to define, significantly improving accuracy.
Deep Instinct is transforming the industry with its technological innovation, transforming security to a model of prevention. Its deep learning-based cybersecurity solution prevents attacks from entering the enterprise in the first place.

Unlike detection and response-based solutions, which wait for the attack to run before reacting, deep-learning can operate preemptively where files and vectors are automatically analyzed prior to execution. By taking this preventative approach customers are kept protected in zero-time. This is critical in a threat landscape, where real-time is too late.

With a deep learning-based solution, businesses don’t have to play cat and mouse, chasing after potential threats to detect and remEDIATE them; no sandboxes or filtering system are necessary. Businesses can continue as normal, without any operational delays. Files can be accessed immediately as the deep learning algorithms have already determined they are safe.

**AN INNOVATIVE APPROACH TO SECURITY**

Deep Instinct uses deep learning as the basis of its cybersecurity solution. Its D-Brain platform uses deep learning algorithms that have been specifically designed for cybersecurity with multiple benefits to be gained.

**Prediction of Unknown Threats**
With the ability to detect any type of activity that distinguishes a malicious threat from normalcy, the product and prevent any kind of threat, known and unknown.

**Zero-Time Detection and Prevention**
The pre-execution approach to threat prevention, followed by detection and remediation and then analysis and remediation, ensures that attacks are identified and blocked before any damage can be caused.

**Zero-Time Classification**
Analysis of enormous amounts of data automatically detects any type of anomaly, classifying malware in zero time with unparalleled accuracy.

**Any Device, Any Operating System, Any File**
The algorithm’s system agnostic design means that every endpoint, server, mobile device, network and operating system is protected against any type of attack, be it fileless or file based.

**Connectionless Edge Deployment**
The deep learning prediction model can be deployed on edge devices as efficient, lightweight client software.

**THE CLICHÉ IS TRUE – AN OUNCE OF PREVENTION BEATS A POUND OF CURE.**
Stepping threats before they become an issue literally saves millions in operational downtime, lost business, mitigation effort, fines and customer defection.

**Conclusion**
The deep learning neural network autonomously applies its predictive determination to prevent threats from entering the enterprise. Through the application of deep learning, Deep Instinct has shown that it is not only possible to prevent threats, but do so, with unparalleled efficacy.

The many benefits in applying deep learning to cybersecurity, but principally it saves the enterprise considerable costs and resources from no longer having to contend with the collateral damages of an attack. The highly accurate and automated solution reduces the pressure on the SOC team, lowering personnel demands and removing alert fatigue. Time and computing resources are not sacrificed to the disastrous fallout of a breach. And business continuity is blissfully assured.

**About Deep Instinct**
Founded in 2015, Deep Instinct provides comprehensive protection against the most evasive known and unknown malware in zero-time, across an organization’s endpoints, servers and mobile devices. Beyond protecting consumers, small and medium businesses and Fortune 500 companies, Deep Instinct utilizes its deep learning capabilities to offer innovative ways to protect and prevent unwanted or targeted systems at attack. With new partnerships expanding every day, Deep Instinct is the first vendor with a patented deep learning cybersecurity framework to block malware attacks from entering the enterprise.

Deep Instinct is led by a highly experienced and interdisciplinary team of deep-learning scientists and Ex-IDF intelligence cyber units. This combined force is revolutionizing the way deep learning is applied to cybersecurity.