Infopercept

# Machine Learning in Future of Cyber Security

Infopercept

# Definition

- At its simplest level, machine learning is defined as “the ability (for computers) to learn without being explicitly programmed.”
- Using mathematical techniques across huge datasets, machine learning algorithms essentially build models of behaviors and use those models as a basis for making future predictions based on newly input data.
- Machine learning is a branch of artificial intelligence (AI) that refers to technologies that enable computers to learn and adapt through experience. It emulates human cognition

Infopercept

# What ML tools need to implement

**ML-powered cyber security tools by comprehending the following**:

- The most important actions and security applications of main machine learning (ML) algorithms.
- How to pick out the most suitable ML algorithm training methods.
- How to scrutinize a security threat detection and ML algorithms' development lifecycle.
- ML cases for attacker behavior detection.

Infopercept

# ML is a dual-use technology

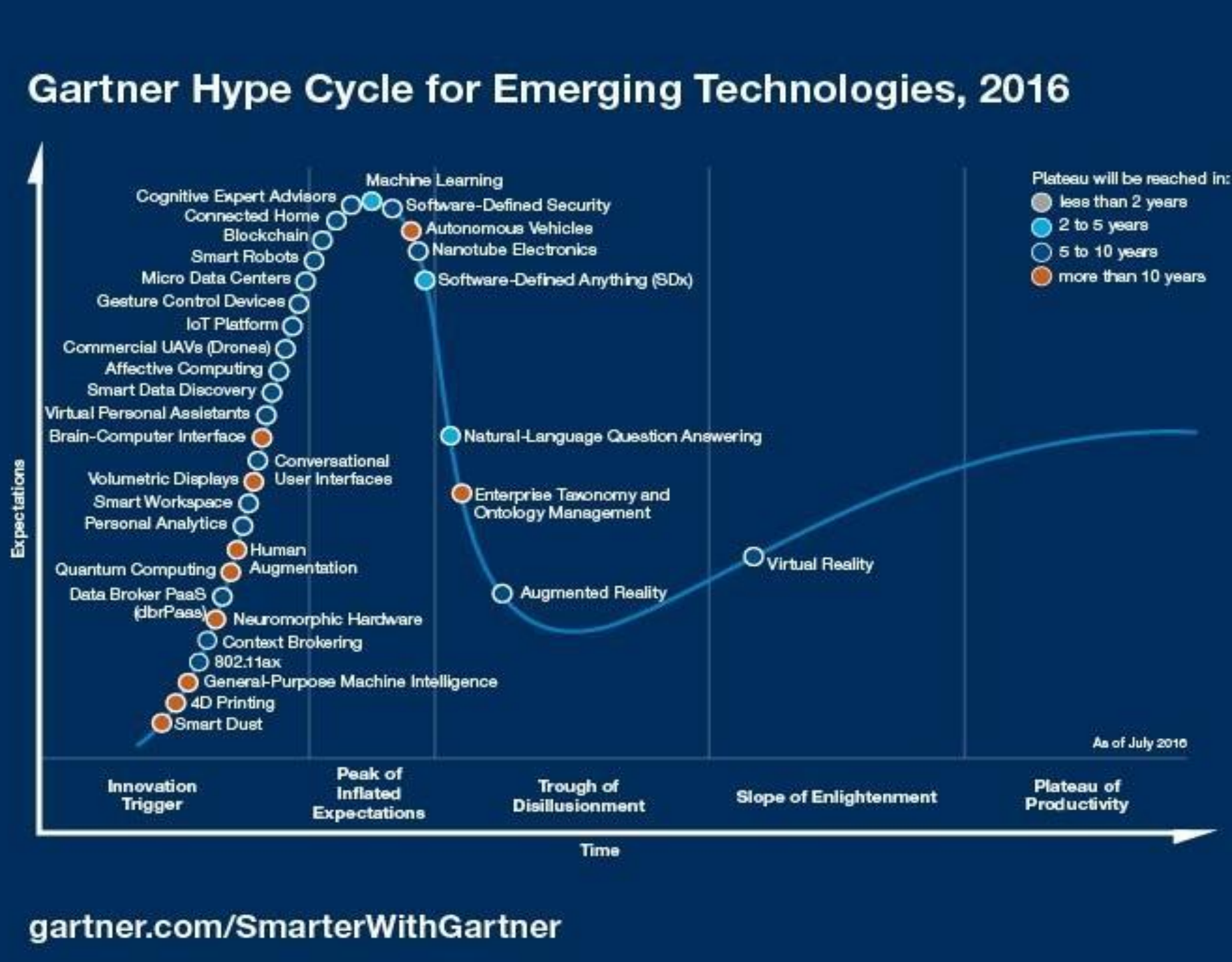
Automation is the name of the game in security and machine learning is here to help. AI is all about automating expert systems, and security is all about experts answering some form of the question:

- Does this matter?
- Does this alert matter?
- Is this vulnerability risky?

Machine learning will help filter out the noise, so that the limited number of practitioners out there can use their time most efficiently

Infopercept

This figure shows Machine Learning is one of the top trending technologies and most expected technology within two to five years in the upcoming future.



Infopercept

# How ML will Affect Cyber Security

## Pattern Recognition

One can’t simply turn on an AI system and expect it to add a strong layer of defense to your network and software. That’s because machine learning is all about taking data from the past and using it to your benefit in the future.

ML algorithms needs information to set a baseline of normal performance and then calculate new events from there. These patterns help the machine learning system to recognize a hacker or a threat to the system.

## Cloud Integration:

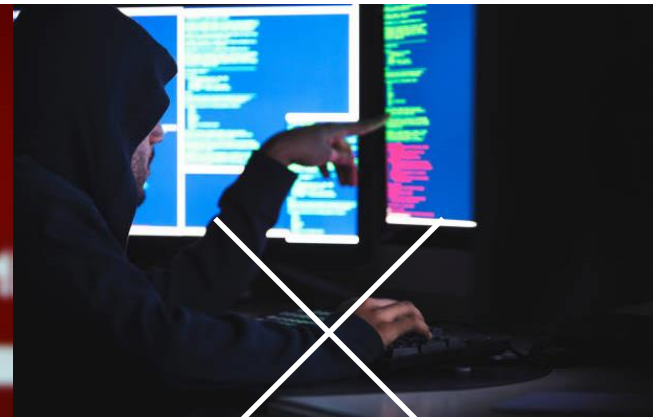
With machine learning intelligence watching over their systems, business of all sizes can secure their cloud environments and protect against the most typical means of malware penetration. It would be wise not to take the word of your cloud provider that they have top-of-the line security in place on the.

## Human Interaction:

Machine learning systems are getting better at natural language processing and trend analysis, but at the end of the day, humans can still do a better job of interpreting spoken and written text.

Infopercept

# Cyber Security threats that machine learning can protect against

## Webshell:

Webshell is a piece of code which is maliciously loaded into a website in order to allow the attacker to make modifications on the web root directory of the server.

From stats machine learning models can be trained to identify normal behavior from malicious behavior. Identified malicious files can be executed on a monitored standalone system in order to train the model further.

## Ransomware:

Neural networks and deep learning algorithms can detect unknown ransomware if data sets can be trained to properly analyze micro behaviors of ransomware attacks.

The task of the algorithm is to find some key features for each file in the data set.

## Spear phishing:

Training predictive URL classification models which are based on latest machine learning algorithms that can identify patterns that reveal a malicious sender's emails.

The models are trained to identify micro behaviors (key features) such as email headers, subsamples of body-data, punctuation patterns, etc. So, these trained models can be used to detect whether the email is malicious or not.

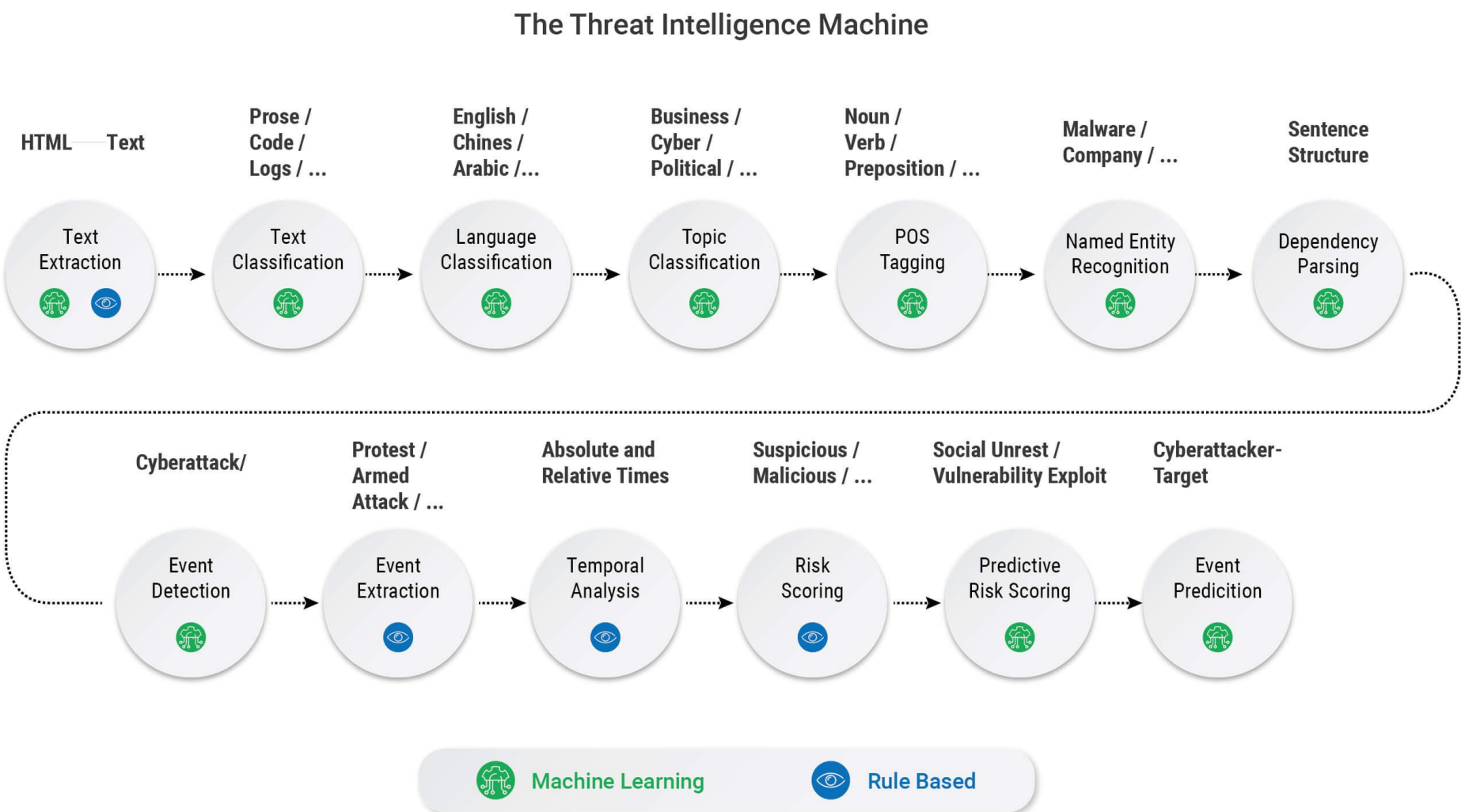
## Watering hole:

Hackers are going to track the sites that users visit often and are external to a user's private network.

Machine learning path traversal detection algorithms can be used to detect these malicious domains. Machine learning can also monitor for rare or extraordinary redirect patterns to and from a site's host.

Infopercept

# Threat Intelligence using ML




# Use Cases

- Using machine learning to detect malicious activity and stop attacks
- Using machine learning to analyze mobile endpoints
- Using machine learning to enhance human analysis
- Using machine learning to automate repetitive security tasks
- Using machine learning to close zero-day vulnerabilities

Infopercept

# THANK YOU

For More Information Please Visit our Website

www.infopercept.com