

# Artificial Intelligence, Machine Learning for Cyber Security Operations


Mark Snyder

Sr Security Specialist Juniper Networks

CISSP, CEH, CISM, CISA

[www.linkedin.com/in/m-snyder](http://www.linkedin.com/in/m-snyder)

# Agenda

- Overview and terms
- What is Artificial intelligence & Machine Learning how are they different
- Benefits of AI/ML
- Demo Machine Learning and Malware 
- Challenges with AI/ML (A Red Team perspective )
- Demo of hacked Machine Learning
- Human Element

# Why this presentation

- I was curious? The great Oz?
- Many IT solutions offer AI / ML but what is it and why is it important
- Set a goal, learn something new!
- CPE credits for me too ;-)
- Spoiler alert     **Its all just math!**

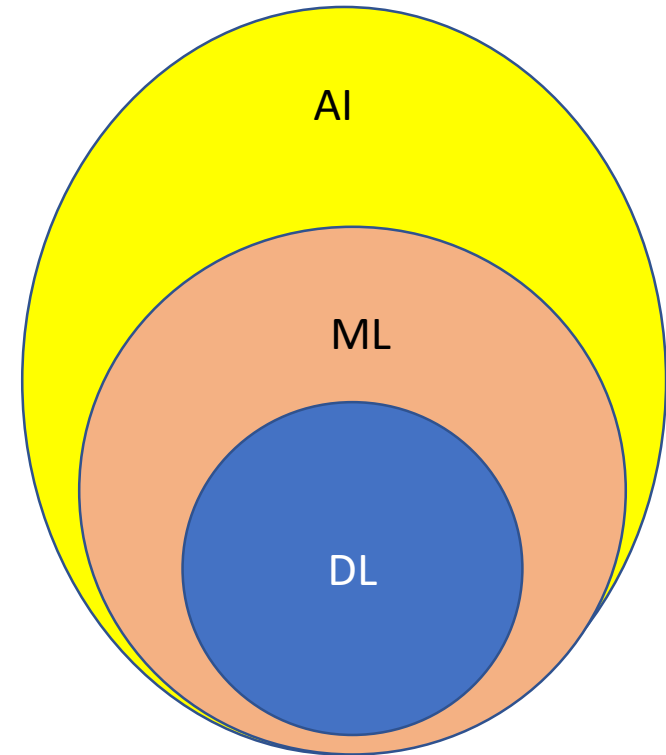
# AI / ML

- AI (Artificial Intelligence)
- ML (Machine Learning)
- DL ( Deep Learning )

AI  $\neq$  ML

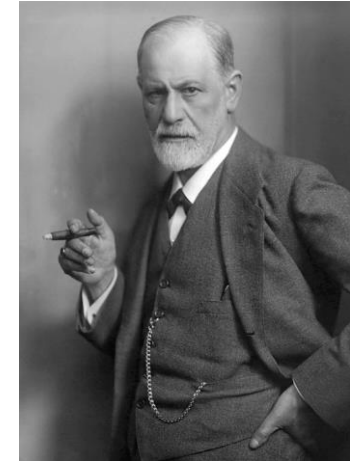
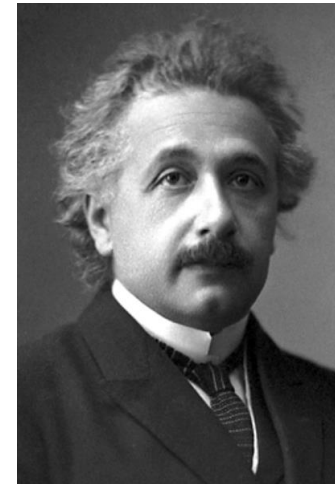
or

AI = ML



# What is AI

- AI 1950s...
  - Definition of ...
  - Turing test...
- Strong AI
- Weak AI
- Expert Systems 1970 80s
- AI Winter /- AI Hype



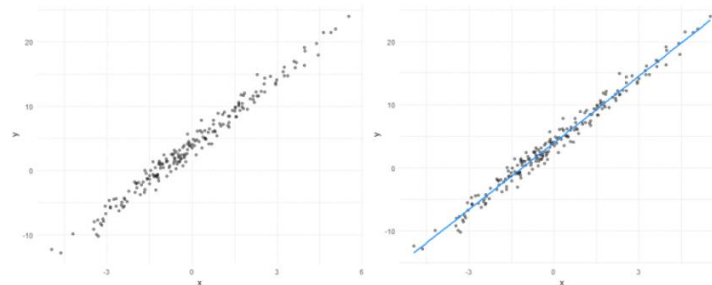
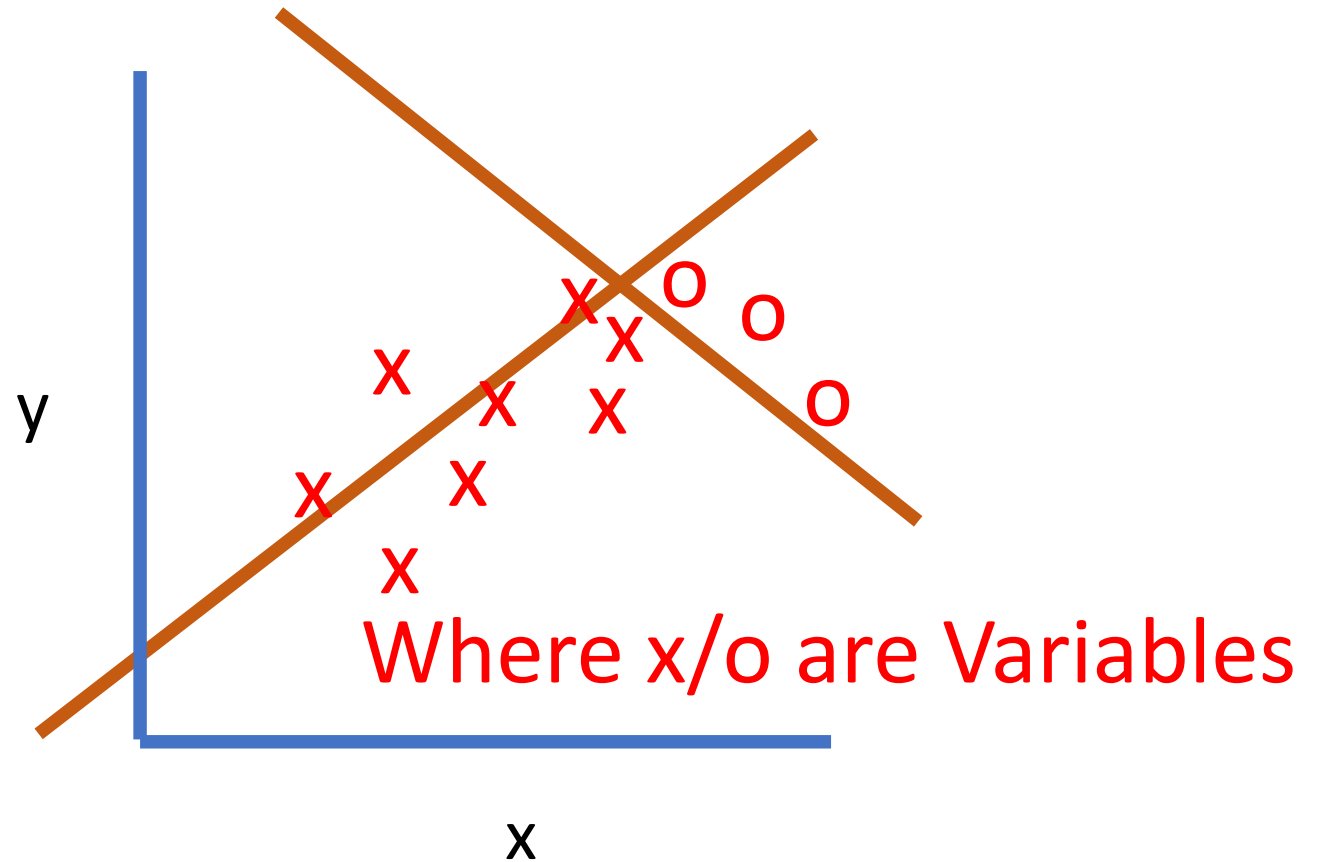
# What is ML

- Definition of...
- High level of how it works
  - Looking for patterns in a data set
  - Based on those patterns make a prediction
  - Those predictions can generate numeric values or class values
- A best guess!
- Linear Algebra / Regression analysis
- Fred Explains it best
- Several approaches
  - Supervised learning
  - Reinforcement learning
  - Unsupervised learning



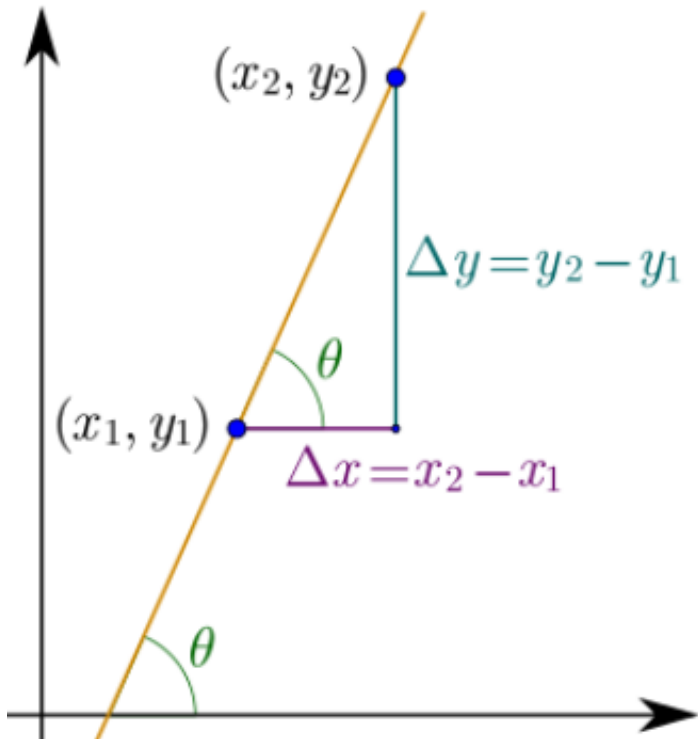
# Supervised ML

- We already know the answer we want! How do we get there...
  - Classification
    - The answer is 42 but how did we get there? 😊
    - An inferred function!
  - Regression
    - $h(x) = (\theta_0 + \theta_1) x$

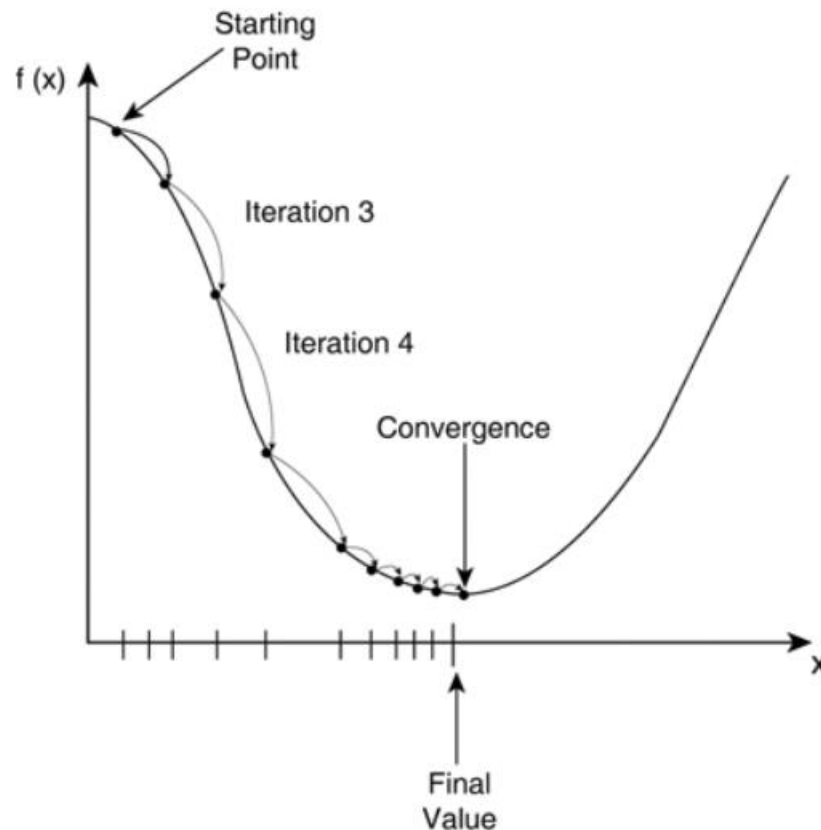


# Supervised ML cont.

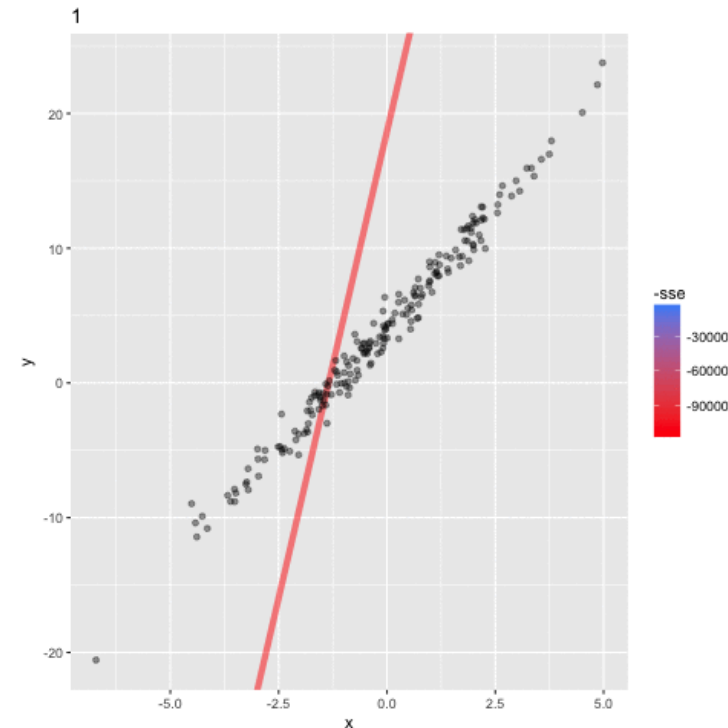
$h(x) = (\theta_0 + \theta_1)x$  What is the slope of  $(\theta_0 + \theta_1)$  compared to  $x$  where the slope has the least cost (aligns closest to the data)



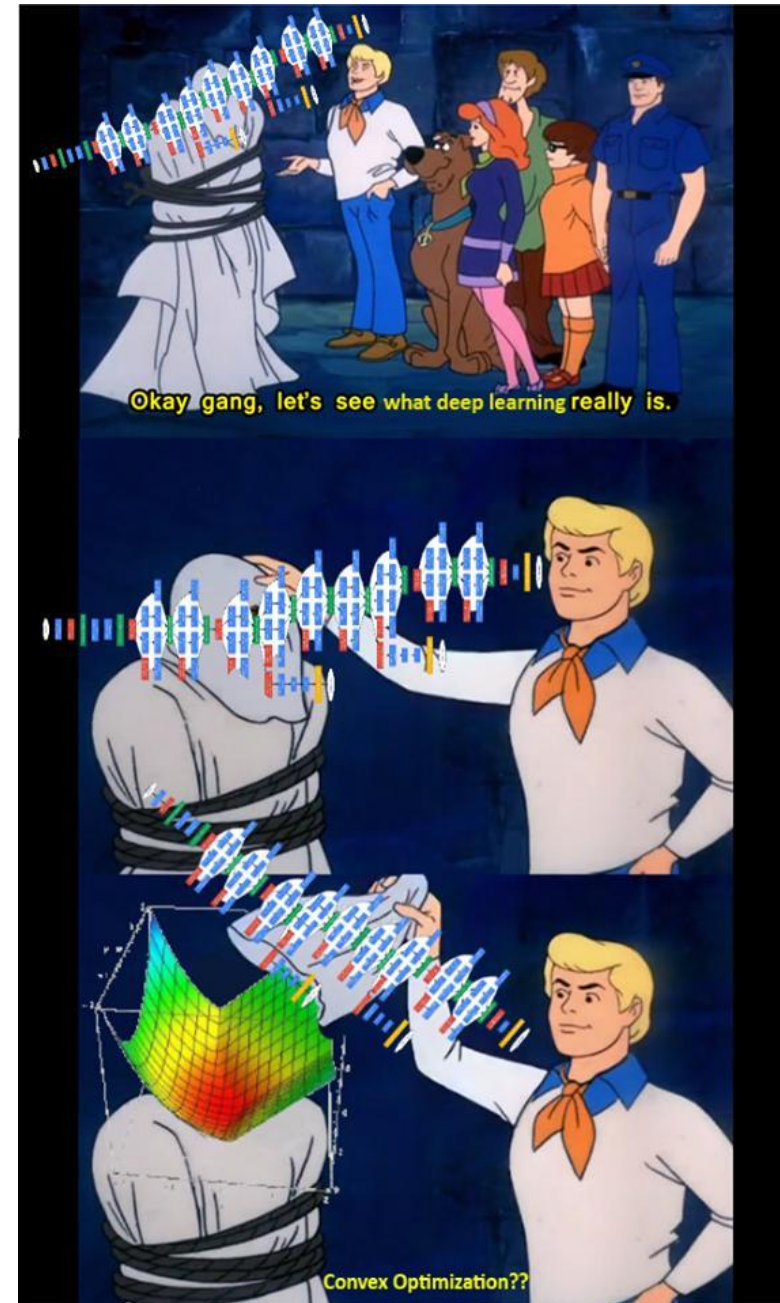
gradient descent algorithm



Model learning



# Supervised ML cont.

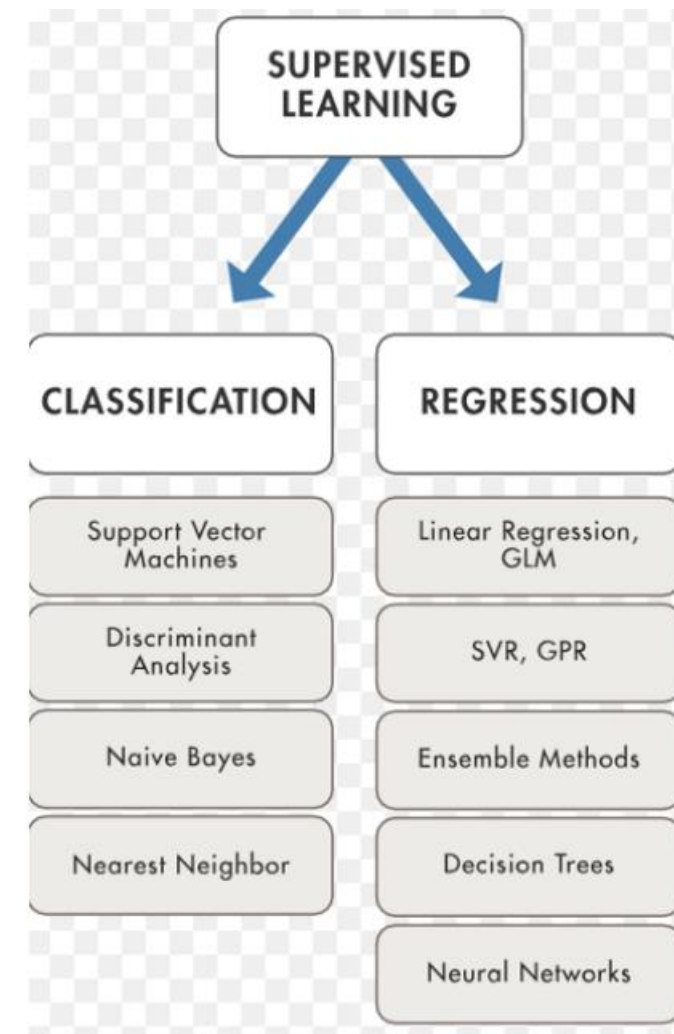


<https://medium.com/@jorgesleonel/supervised-learning-c16823b00c13>

<https://devrant.com/rants/639361/what-deep-learning-really-is>

# ML - Classification / Regression Methods

- Decision trees
- Ensembles ( Bagging, Boosting, Random forest )
- k-NN
- Linear regression
- Naive Bayes
- Artificial neural networks
- Logistic regression
- Perceptron
- Relevance vector machine (RVM)
- Support vector machine (SVM)



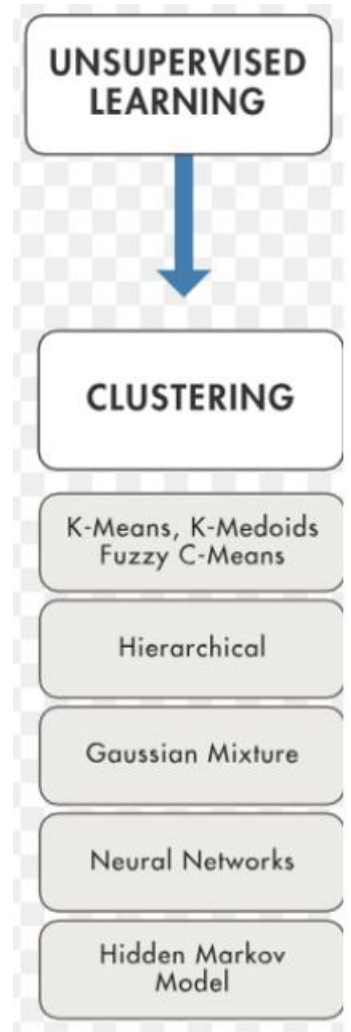
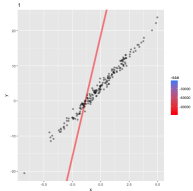
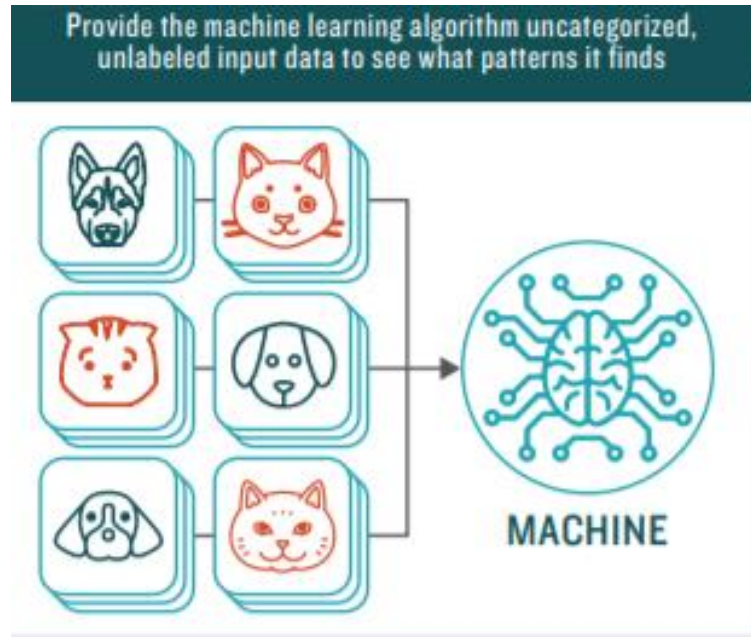
# Regression Learning

- Rewards based learning
  - Agent
    - Deliberate approach
    - Trial an error
    - Negative and positive reinforcement



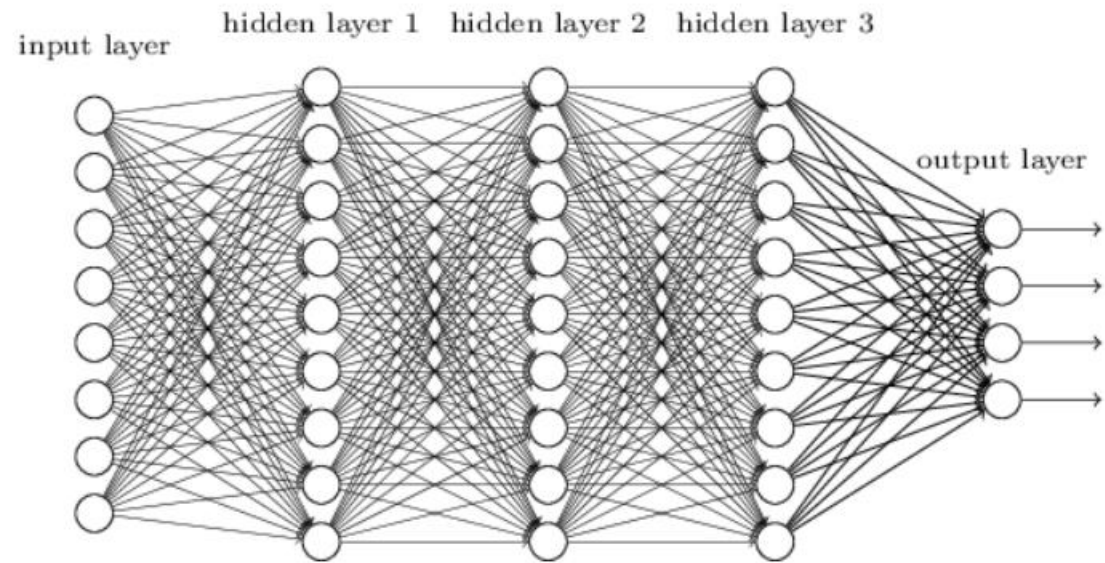
# Unsupervised ML

- Gray input



# Neural Networks / Deep learning

- Is a subset of Machine Learning
- Moreover can be:
  - Supervised learning
  - Reinforcement learning
  - Unsupervised learning



# ML Benefits



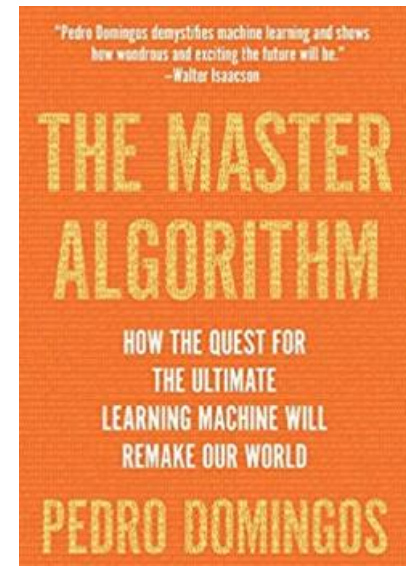
# Were Machine learning can benefit IT

- Cyber operations
  - Fatiguing amount of log data
  - Grueling amount of attributes
  - Knowledge needed (depth and breadth)
  - Experience needed



# Benefits of Machine learning in IT Operations

- Hypothesis  $h(x) = (\theta_0 + \theta_1) x$ 
  1. Anything that can be observed and documented (logged),
  2. Have a labeled value (input),
  3. Can be checked for clustering (grouping), classified or linear comparison.
- However, keep in mind:
  - Not all data sets lend themselves to all ML algorithms (There is no master Algorithm)
  - Not everything has an answer

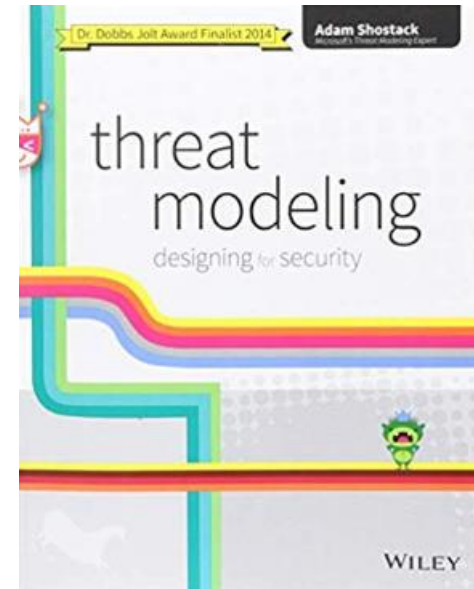


# Benefits

- What are my attack surfaces?
- How can I collect data from them?

Nouns  $\approx$  Attack Surfaces (AS)

$AS_{(0-100...)} = Risk_{(0-100...)}$



# Tools

- University of California



## Machine Learning Repository

Center for Machine Learning and Intelligent Systems

[View](#)

### Welcome to the UC Irvine Machine Learning Repository!

We currently maintain 481 data sets as a service to the machine learning community. You may [view all data sets](#) through our searchable interface. For a general overview of the Repository, please visit our [About page](#). For information sets in publications, please read our [citation policy](#). If you wish to donate a data set, please consult our [donation policy](#). For any other questions, feel free to [contact the Repository librarians](#).

Supported By:  In Collaboration With: 

#### Latest News:

**09-24-2018:** Welcome to the new Repository admins Dheeru Dua and Efi Karra Taniskidou!

**04-04-2013:** Welcome to the new Repository admins Kevin Bache and Moshe Lichman!

**03-01-2010:** [Note](#) from donor regarding Netflix data








**10-16-2009:** Two new data sets have been added.

**09-14-2009:** Several data sets have been added.








**03-24-2008:** New data sets have been added!

**06-25-2007:** Two new data sets have been added: UJI Pen Characters, MAGIC Gamma Telescope


#### Newest Data Sets:

07-30-2019:		<a href="#">PPG-DaLiA</a>
07-24-2019:		<a href="#">Divorce Predictors data set</a>
07-22-2019:		<a href="#">Alcohol QCM Sensor Dataset</a>
07-14-2019:		<a href="#">Incident management process enriched event log</a>
06-30-2019:		<a href="#">Wave Energy Converters</a>
06-22-2019:		<a href="#">Query Analytics Workloads Dataset</a>
06-17-2019:		<a href="#">Opinion Corpus for Lebanese Arabic Reviews (OCLAR)</a>

#### Most Popular Data Sets (hits since 2007):

2766045:		<a href="#">Iris</a>
1553966:		<a href="#">Adult</a>
1204694:		<a href="#">Wine</a>
1019372:		<a href="#">Car Evaluation</a>
994890:		<a href="#">Wine Quality</a>
982949:		<a href="#">Heart Disease</a>
974481:		<a href="#">Breast Cancer Wisconsin (Diagnostic)</a>

#### Featured Data Set: [Balance Scale](#)



**Task:** Classification  
**Data Type:** Multivariate  
**# Attributes:** 4  
**# Instances:** 625

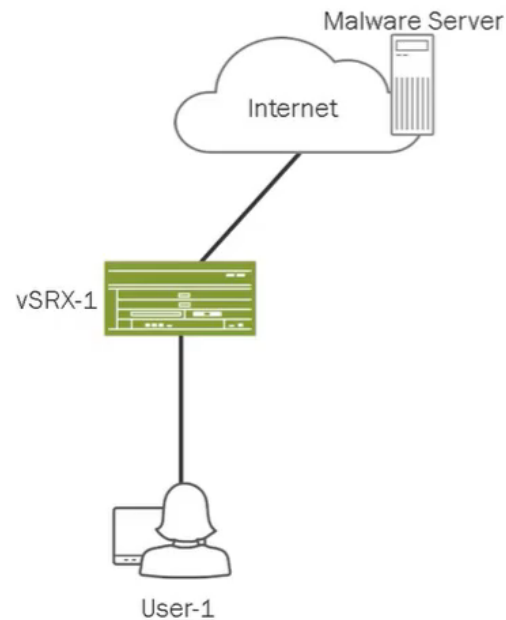
# Tools cont.

- MATLAB
- Octave
- Python
- R
- C++
- .....



# ML working demo

## Sky ATP Web Protection – CLI



### ■ Criteria for example

- vSRX-1 already enrolled with Sky ATP
- Block ...
  - Malicious files downloaded through HTTP
  - Users from communicating through vSRX-1 if they download malicious files through HTTP

# ML Challenges



# Challenges with ML / AI

- Greedy
- Fragile
- Biases
  - Learned
  - Goals
  - Narrow w/support



# Red Teaming (Hacking ML)

- Attack surfaces

- Model

- Algorithms
    - Parameters

} Model Abstraction Attacks... Prediction APIs

- Data

- Training and testing sets
    - Deployed environment data

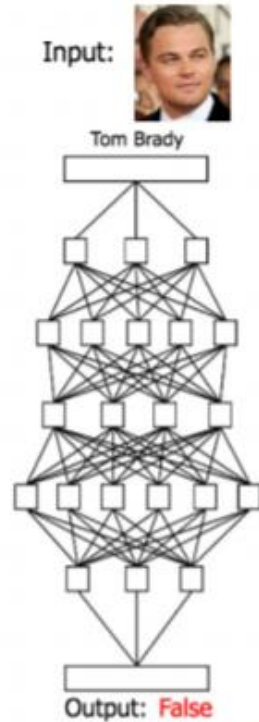
} Poisoning

# ML Adversarial attacks examples

- Example 1
  - Modifying data
- Example 2
  - Tricking Classification
- Example 3
  - Invisibility

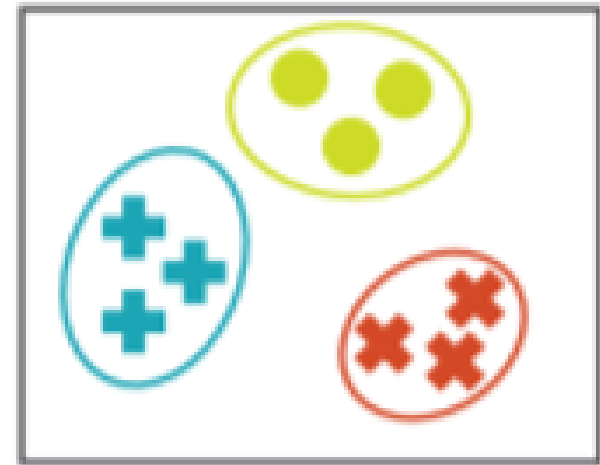
# Example 1 - Modifying data

- Backdooring Convolutional Neural Networks via Targeted Weight Perturbations



# Example 2 - Tricking Classification

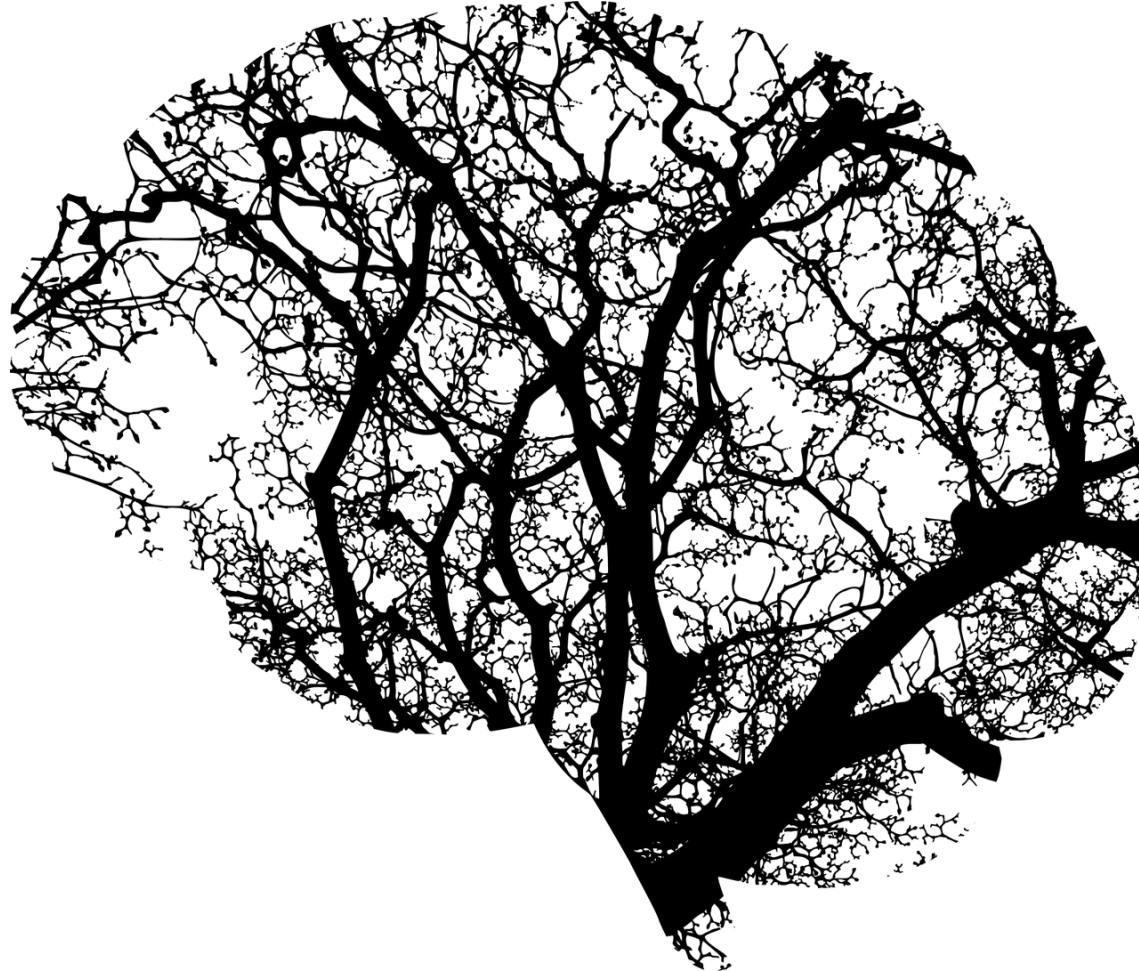
- Blacklisting
- Whitelisting
- Predicting APIs with Model abstractions



# Example 3 - ML Invisibility



# Human Element



# Human Element

- When something goes right or wrong
- Ownership
- Responsibility
- Positive & Negative



# Closing comments

- Wish I had more time
- Still learning myself, and looks like so is everyone else...
- Lots of surface level info
- Good info is out there just hard to find
- What I would have done differently

*Q&A*

*fin*

Thank you - Mark  
[www.linkedin.com/in/m-snyder](http://www.linkedin.com/in/m-snyder)

# References

Machine learning for Beginners, Travis Goleman, Independently published - February 12, 2019

Wikipedia contributors. (2019, July 24). Deep learning. In Wikipedia, The Free Encyclopedia. Retrieved 17:33, August 13, 2019, from [https://en.wikipedia.org/w/index.php?title=Deep\\_learning&oldid=907716010](https://en.wikipedia.org/w/index.php?title=Deep_learning&oldid=907716010)

Wikipedia contributors. (2019, June 11). Statistical classification. In *Wikipedia, The Free Encyclopedia*. Retrieved 01:07, August 14, 2019, from [https://en.wikipedia.org/w/index.php?title=Statistical\\_classification&oldid=901384363](https://en.wikipedia.org/w/index.php?title=Statistical_classification&oldid=901384363)

Artificial intelligence for dummies, John Mueller-Luca Massaron - John Wiley & Sons, Inc. – 2018

<https://medium.com/@jorgesleonel/supervised-learning-c16823b00c13>

<https://www.newtechdojo.com/list-machine-learning-algorithms/>

[https://www.boozallen.com/content/dam/boozallen\\_site/sig/pdf/publications/machine-intelligence-quick-guide-to-how-machines-learn.pdf](https://www.boozallen.com/content/dam/boozallen_site/sig/pdf/publications/machine-intelligence-quick-guide-to-how-machines-learn.pdf)

<https://towardsdatascience.com/machine-learning-fundamentals-via-linear-regression-41a5d11f5220>

Wikipedia contributors. (2019, August 6). Slope. In *Wikipedia, The Free Encyclopedia*. Retrieved 17:17, August 14, 2019, from <https://en.wikipedia.org/w/index.php?title=Slope&oldid=909523667>

<https://arxiv.org/pdf/1904.08653v1.pdf>