MACHINE LEARNING

FUTURE OF CYBERSECURITY?

KARISHMA MEHTA

CS_KARISHMA@YAHOO.COM

AGENDA

- Industry Hoopla
- Machine Learning (ML) Visionaries
- What's Machine Learning?
  - Supervised Learning
  - Unsupervised Learning
- Cybersecurity Attack Landscape
- Possible use cases
- ML Shortcomings
- Conclusion

AGENDA

- Industry Hoopla
- Machine Learning (ML) Visionaries
- What's Machine Learning?
  - Supervised Learning
  - Unsupervised Learning
- Cybersecurity landscape
- Possible use cases
- ML Shortcomings
- Conclusion

INDUSTRY HOOPLA

High accuracy- no noise

No update ever needed

No endpoint protected by our products has ever been breached

Machine Learning and AI – same results as SME

29x better productivity

Automatically detects and classifies

AGENDA

- Industry Hoopla
- Machine Learning (ML) Visionaries
- What's Machine Learning?
  - Supervised Learning
  - Unsupervised Learning
- Cybersecurity Attack Landscape
- Possible use cases
- ML Shortcomings
- Conclusion

ML VISIONARIES

"The development of full artificial intelligence could spell the end of the human race." Hawking

Artificial intelligence could be the "most likely" cause of a third world war. Musk

the nation that leads in AI 'will be the ruler of the world' Putin

"We are at the beginning of the goldern age of Ai" Bezos

AGENDA

- Industry Hoopla
- Machine Learning (ML) Visionaries
- What's Machine Learning?
  - Supervised Learning
  - Unsupervised Learning
- Cybersecurity Attack Landscape
- Possible use cases
- ML Shortcomings
- Conclusion

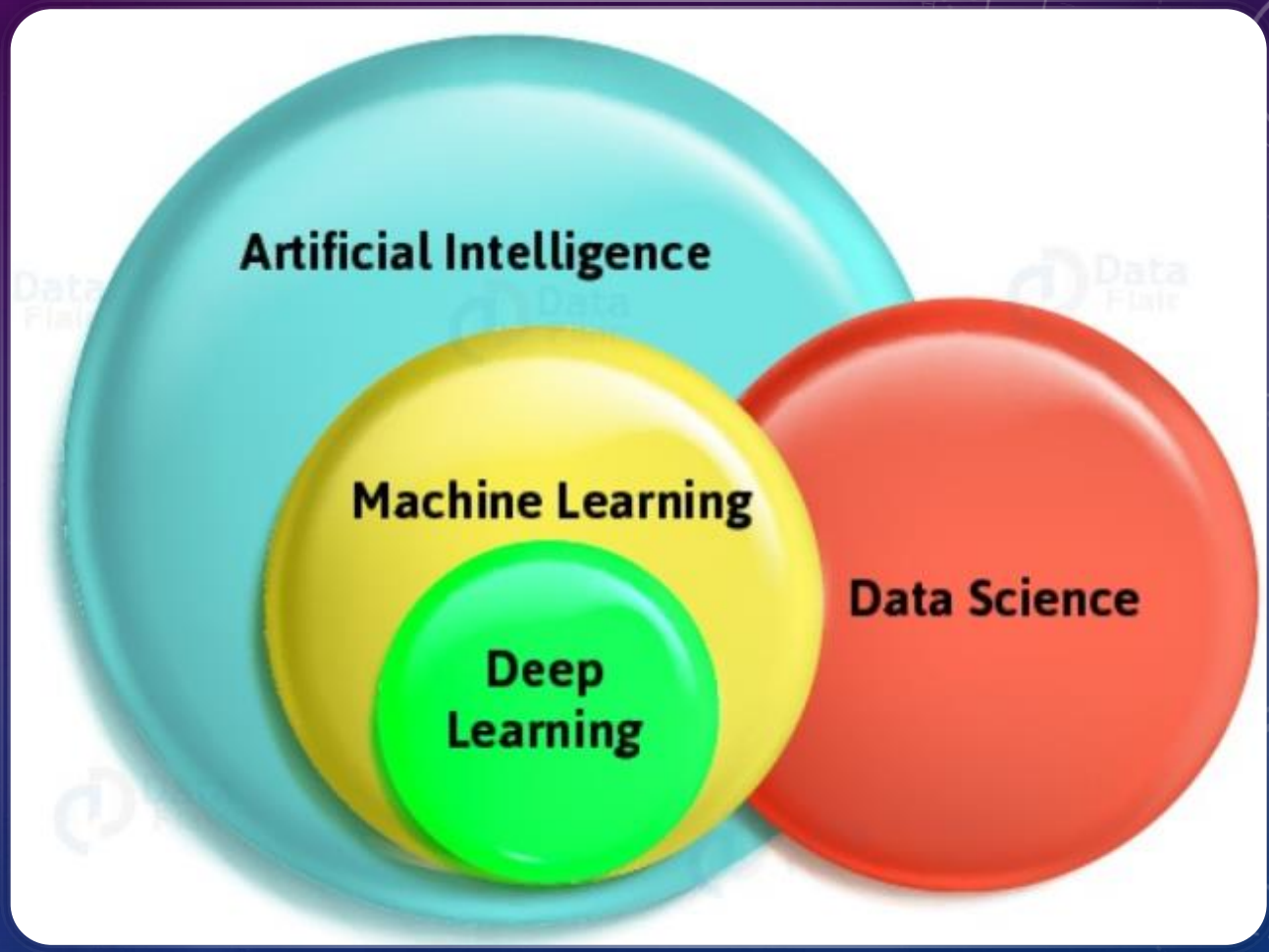
ARTIFICIAL INTELLIGENCE

Artificial intelligence

- If a given machine can interpret the data, learn from it, and use that knowledge to adapt and achieve specific goals

Machine Learning

- If a machine can learn without being explicitly programmed



ML FURTHER DEFINED

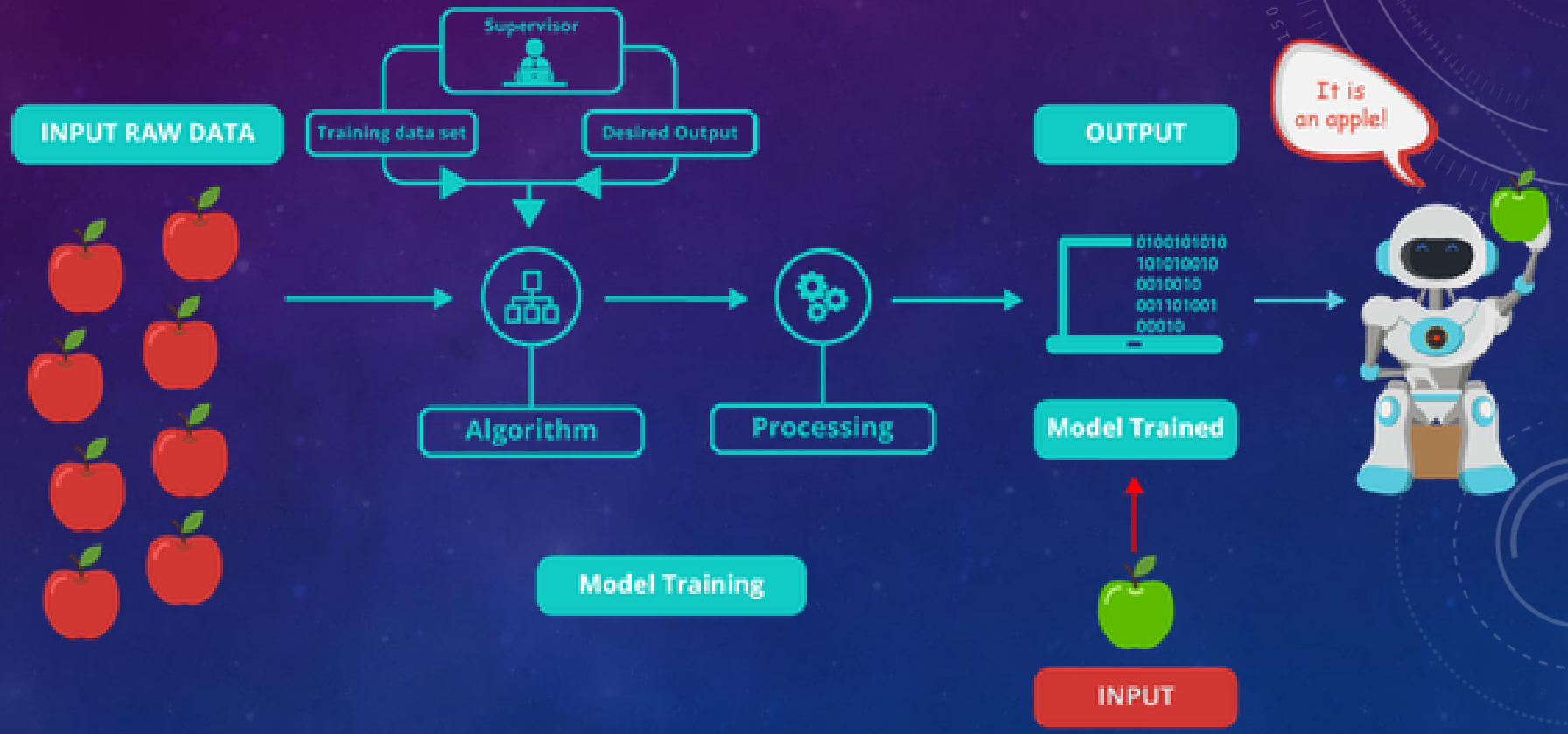
The process by which a computer can improve its own performance by continuously incorporating new data into an existing statistical model (Merriam-Webster)

The hope is that ML can help us with better prediction, classification, prioritization

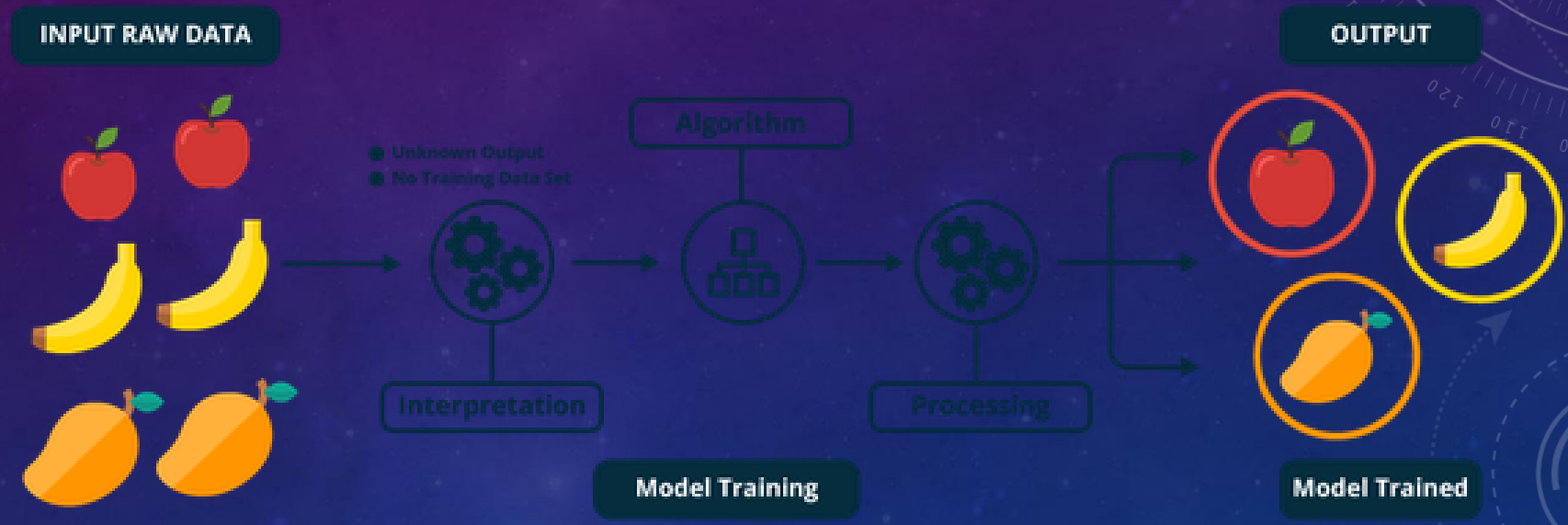
ML (CONT…)


Analytics
Human Input
Descriptive
What happened?
Diagnostic
Why did it happen?
Predictive
What will happen?
Prescriptive
What should I do?
Data
Machine Learning
Decision
Action
Decision Support
Decision Automation

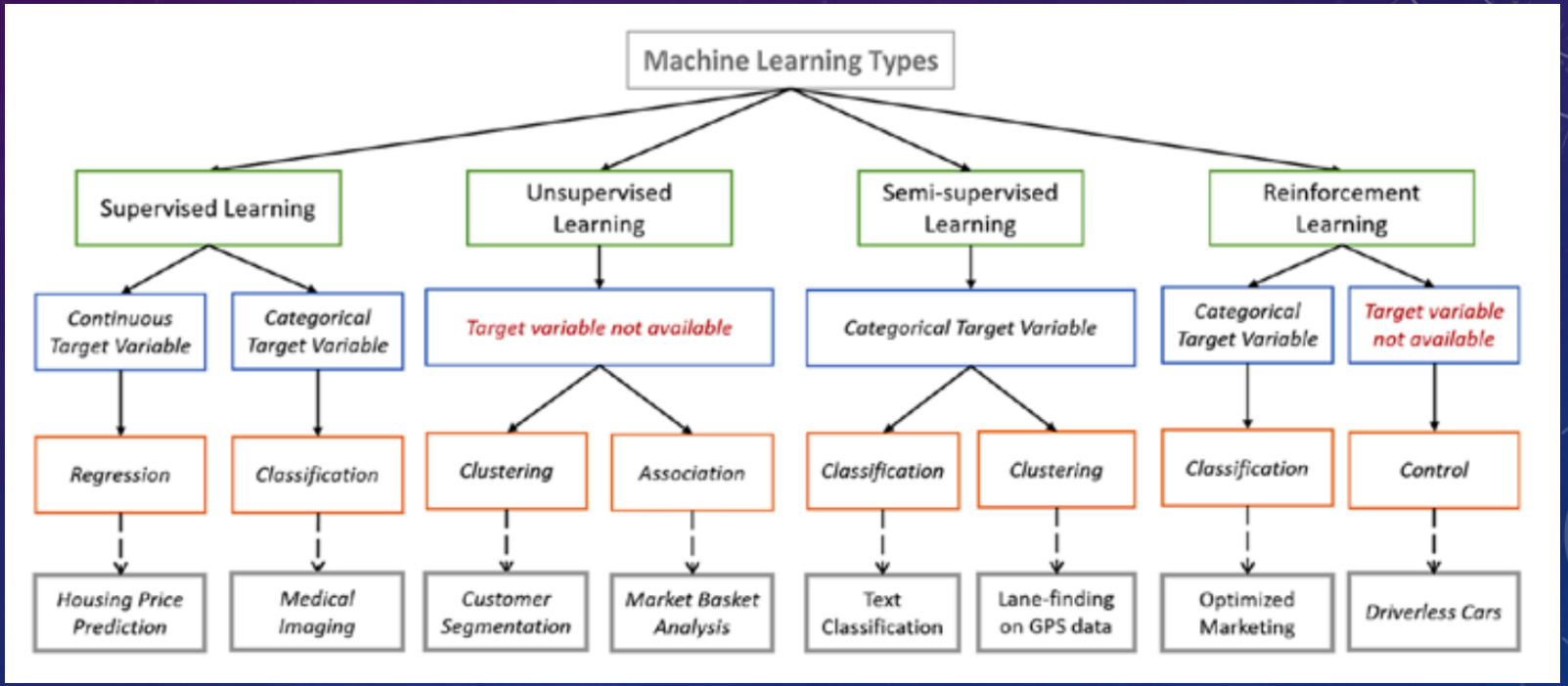
SUPERVISED LEARNING



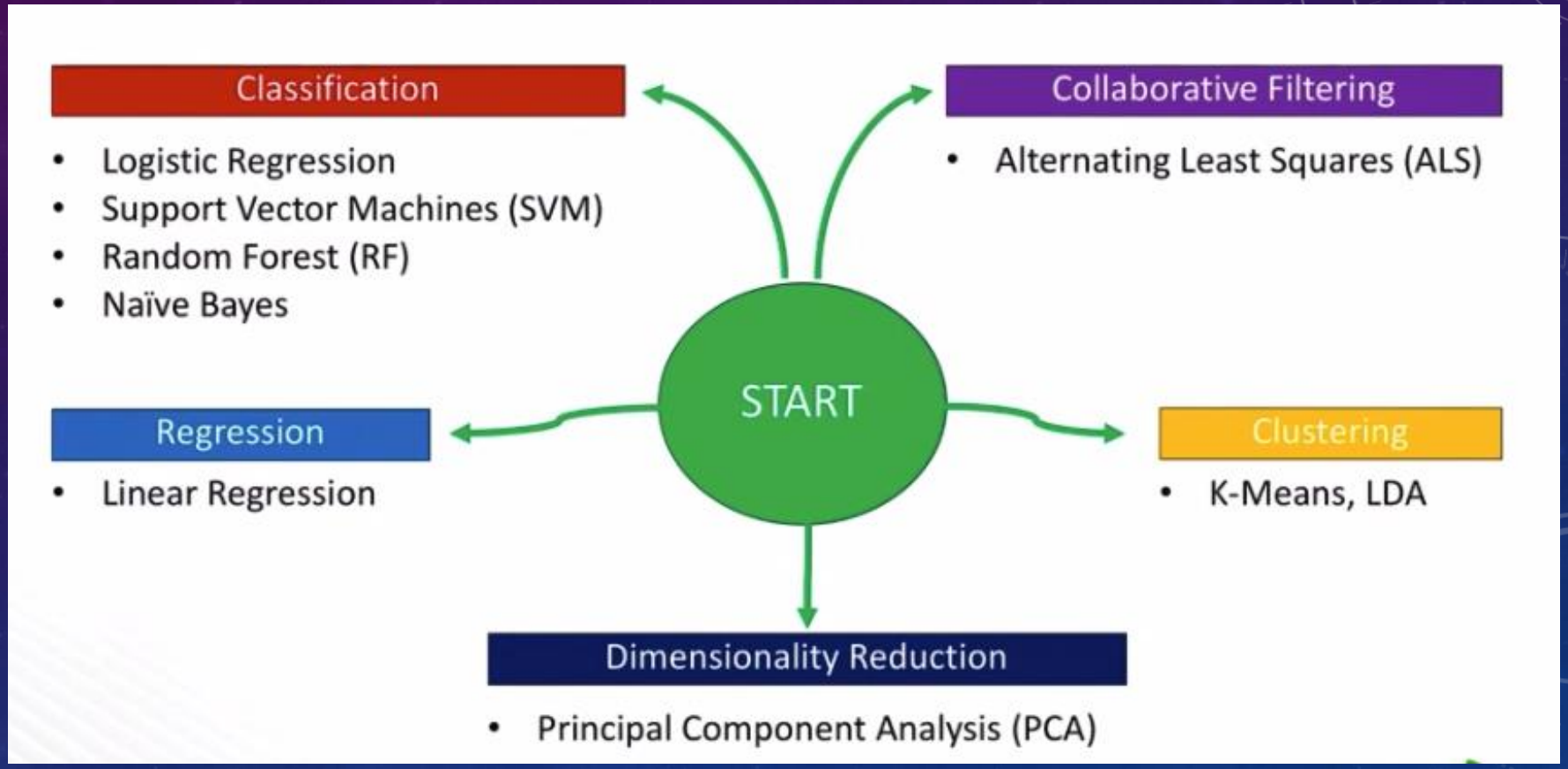
UNSUPERVISED LEARNING



MACHINE LEARNING GENERAL ALGORITHMS



ALGORITHMS (CONT…)

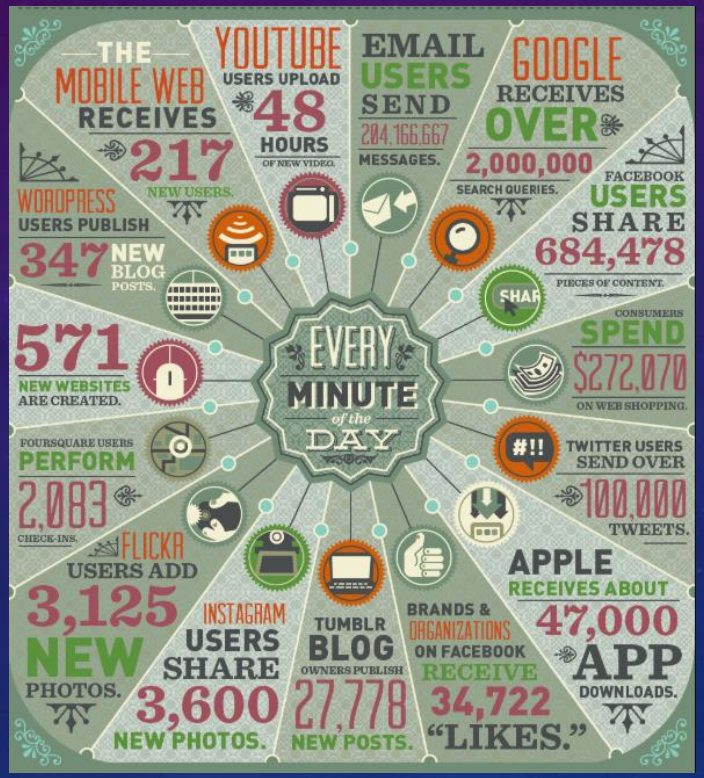


https://medium.com/machine-learning-in-practice/cheat-sheet-of-machine-learning-and-python-and-math-cheat-sheets-a4afe4e791b6

AGENDA

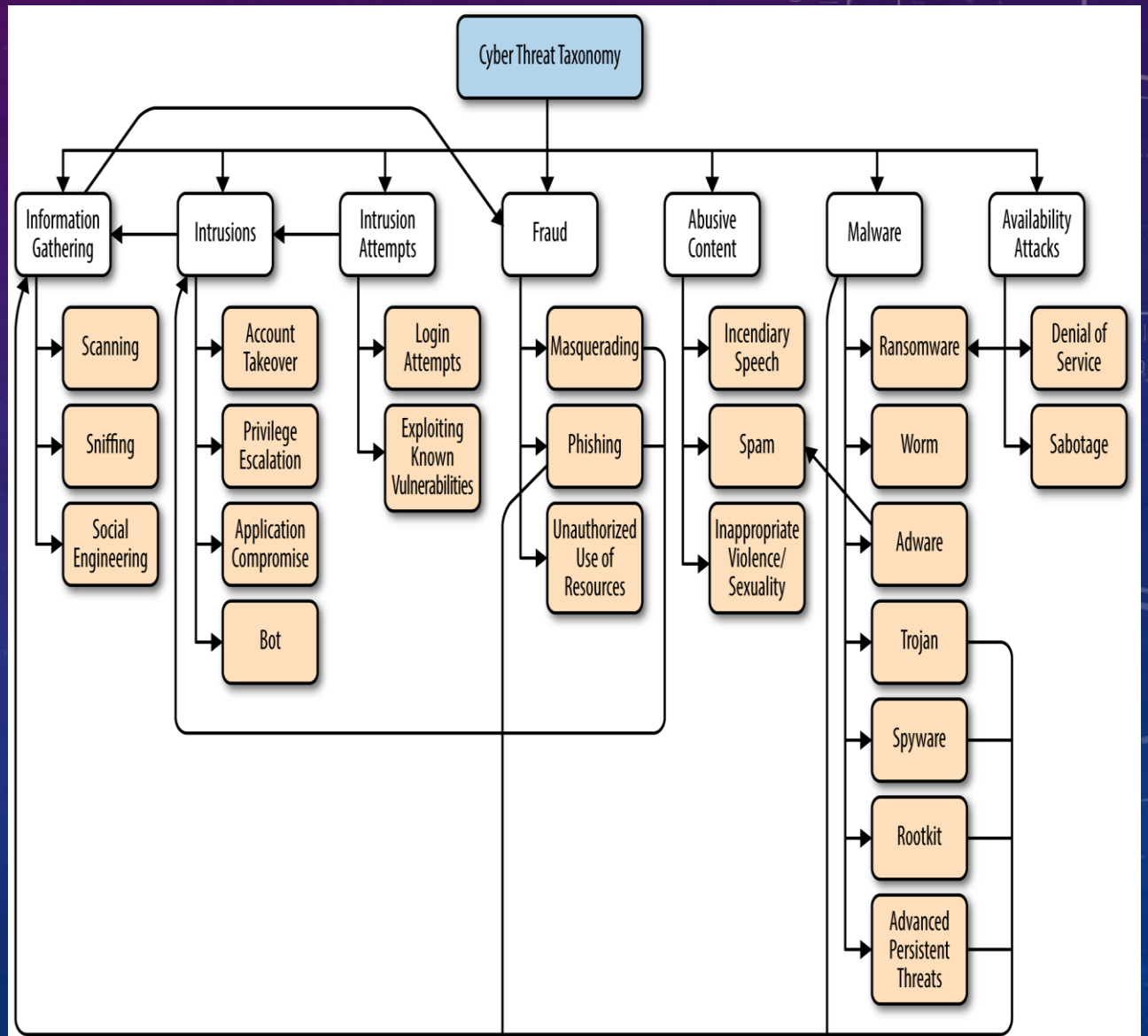
- Industry Hoopla
- Machine Learning (ML) Visionaries
- What's Machine Learning?
  - Supervised Learning
  - Unsupervised Learning
- Cybersecurity Attack Landscape
- Possible use cases
- ML Shortcomings
- Conclusion

DOMO : DATA NEVER SLEEPS



CYBERSECURITY ATTACK LANDSCAPE

- *Prior actions*
- *Occurred actions*
- *Potential actions*
- *Detection Mitigation*
- *Relevant threat actors*
- *Intent*
- *Capabilities*
- *Tactics, techniques and procedures (TTP)*
- *Vulnerable*
- *Misconfigurations*
- *Weaknesses*



DATA MINING

- Classification
- Estimation
- Prediction
- Clustering
- Visualization

CYBER KILL CHAIN

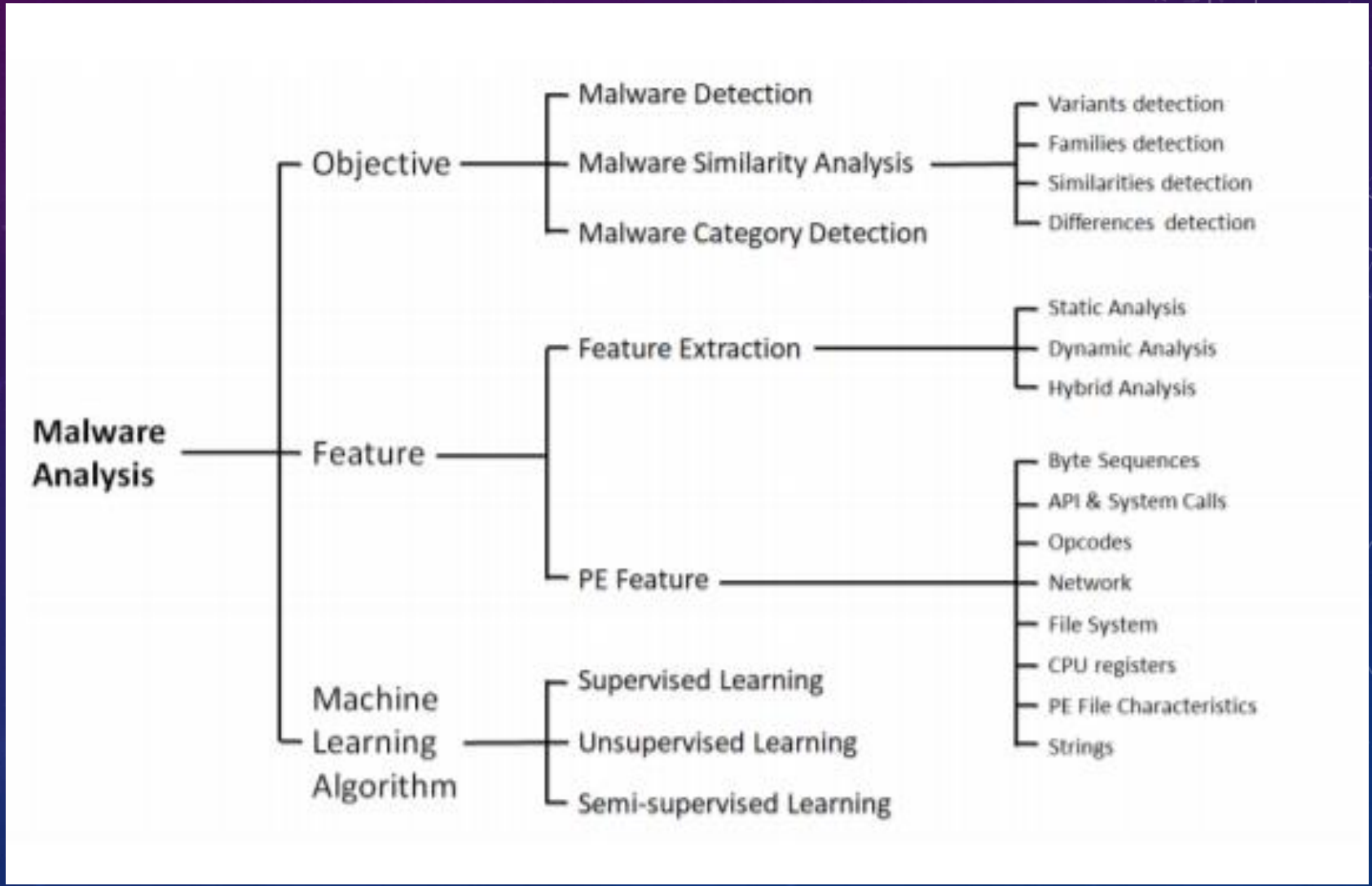
AGENDA

- Industry Hoopla
- Machine Learning (ML) Visionaries
- What's Machine Learning?
  - Supervised Learning
  - Unsupervised Learning
- Cybersecurity Attack Landscape
- Possible use cases
- ML Shortcomings
- Conclusion

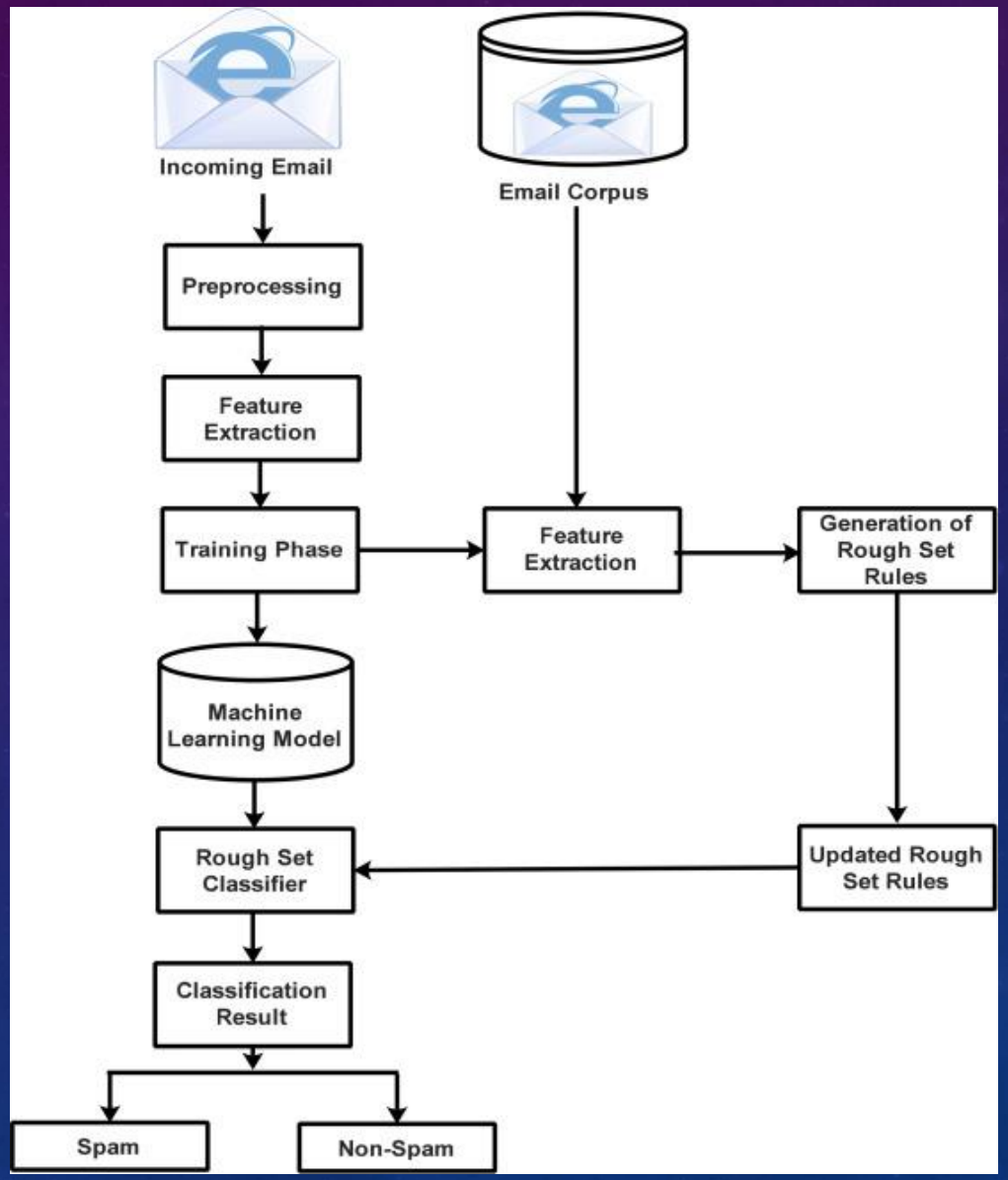
ML USE CASES IN CYBERSECURITY

Network Threat Identification	DLP	Antivirus/ Malware detection	Email/ Chatbot	User Behavior Modeling
ShiledX- identifying which security policies are applicable for each application	Bay Dynamics and Symantec	Smart Antivirus : AI to predict, detect and respond to cybersecurity threats	Knowmail Agari inbenta	Darktrace
Versive - use anomaly detection to identify network security threats		Harvest.AI Macie McAfee, Sophos, Symantec, Trend Micro, Webroot, MobileIron and		

MALWARE DETECTION TAXONOMY



EMAIL SPAM SAMPLE WORKFLOW



THREAT INTELLIGENCE MODEL

https://littlefield.co/cyber-threat-intelligence-applying-machine-learning-data-mining-and-text-feature-extraction-to-bb00c3b729bc

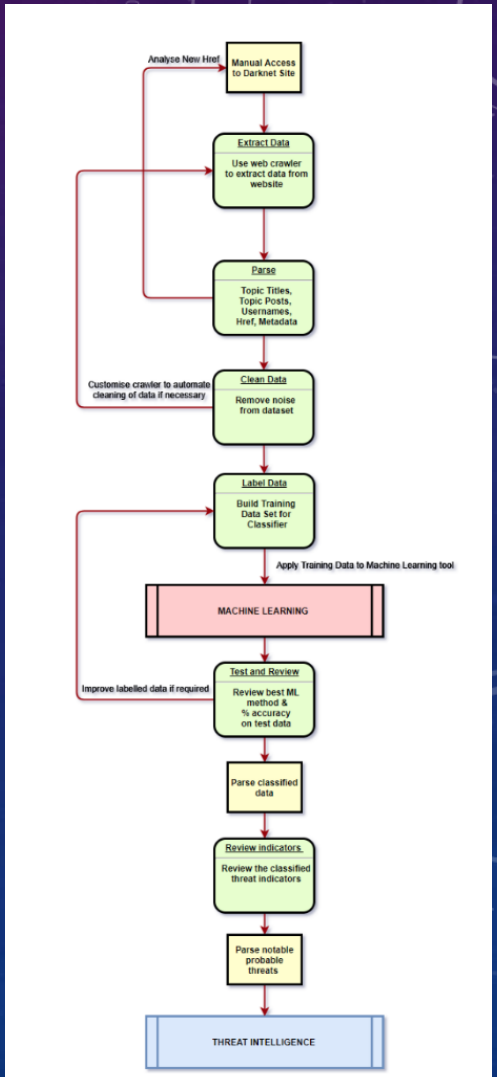


Figure 7: Threat Intelligence Model Overview

AGENDA

- Industry Hoopla
- Machine Learning (ML) Visionaries
- What's Machine Learning?
  - Supervised Learning
  - Unsupervised Learning
- Cybersecurity landscape
- Possible use cases
- ML Shortcomings
- Conclusion

ML SHORTCOMINGS IN CYBERSECURITY

- No standard framework
- Not enough rich data
- Not enough experts per domain
- No standard features set
- Not enough computational power/memory to process ton of data
- Not enough training time
- Not enough customization on blocks & algorithms

AGENDA

- Industry Hoopla
- Machine Learning (ML) Visionaries
- What's Machine Learning?
  - Supervised Learning
  - Unsupervised Learning
- Cybersecurity landscape
- Possible use cases
- ML Shortcomings
- Conclusion

CONCLUSION

Models does not learn on its own

Models does not give us 99% accuracy

Once model is trained, we need to keep retraining with changing situation

Need continuous learning and shifting

Still not at the level of production