MACHINE LEARNING FOR BEING HACKPROOF

By
Sandipan Roy
M.Sc[Semester-3]
Department of Computer Science
West Bengal State University

INTRODUCTION

What is Hacking?

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access.

Who is a Hacker?

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access.

INTRODUCTION(Cont.)

What is Machine Learning(ML)?

- An application of artificial intelligence (AI)
- Provides systems the ability to automatically learn
- Improve from experience without being explicitly programmed

Why We Choose Machine Learning for being Hackproof?

- To detect malicious activity and stop attacks
- To automate repetitive security tasks
- To close Vulnerabilities
- Forensic analysis & Incident response
- Prevention and threat modeling using predictions

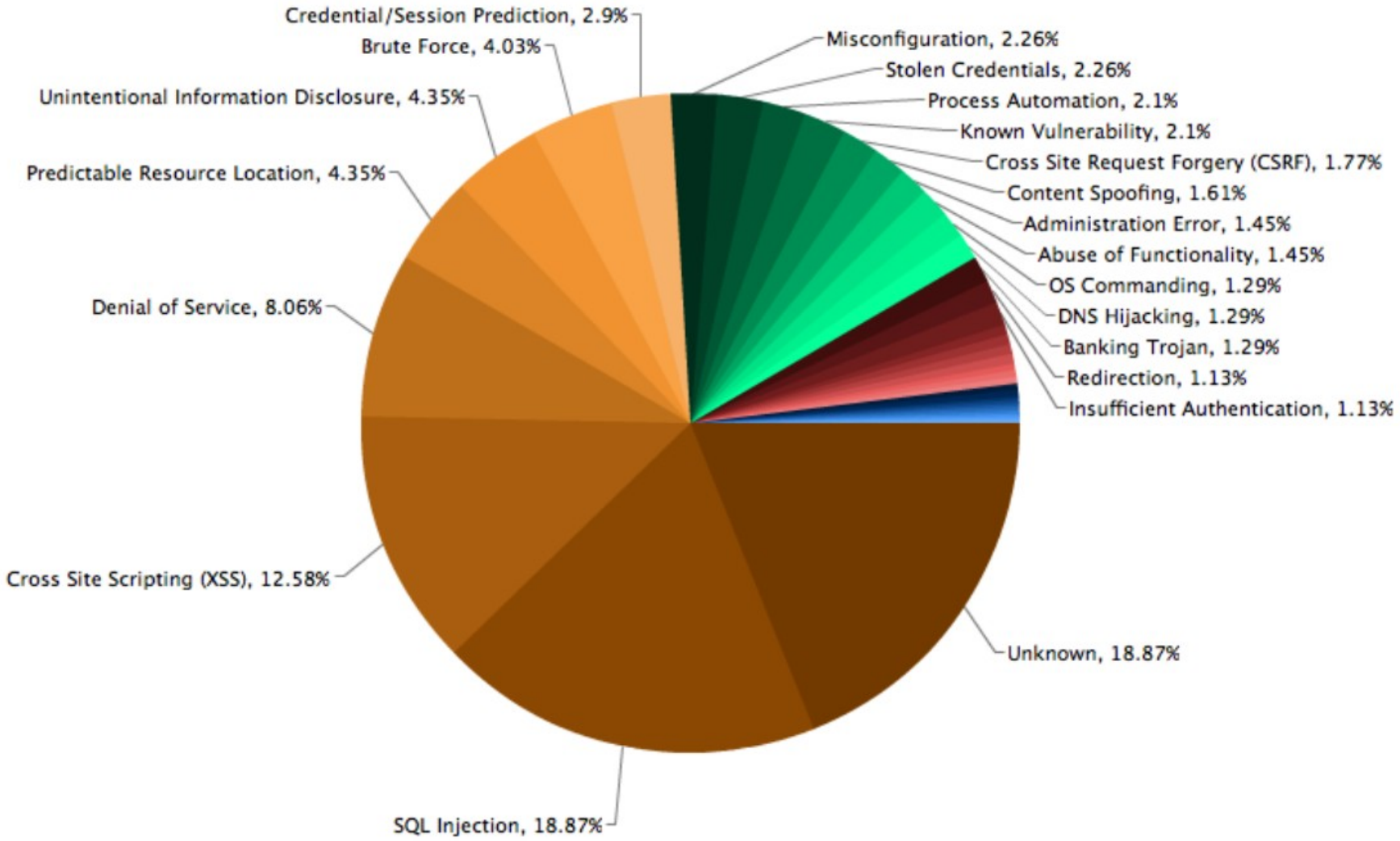
TYPE OF HACKING TECHNICS

- Phishing / Spamming
- Virus / Malware / Ransomware
- SQL Injection / XSS Attack
- Distributed Denial-of-Service (DDoS) Attack
- Rootkit / Backdoors
- Security Misconfiguration/Broken Access Control

STEP BY STEP PROCEDURE TO HACK A USER

- Phishing → Rootkit / Backdoors → Virus / Malware
- SQL Injection → Virus / Malware → Reverse TCP
- Sniffing → Access Control → Backdoors/Malware
- XSS Attack → Found a Vulnerabilities → Malware/Virus
- Man in the Middle → Gain Information
- To Be Continued.....

CYBER ATTACKS STATISTICS

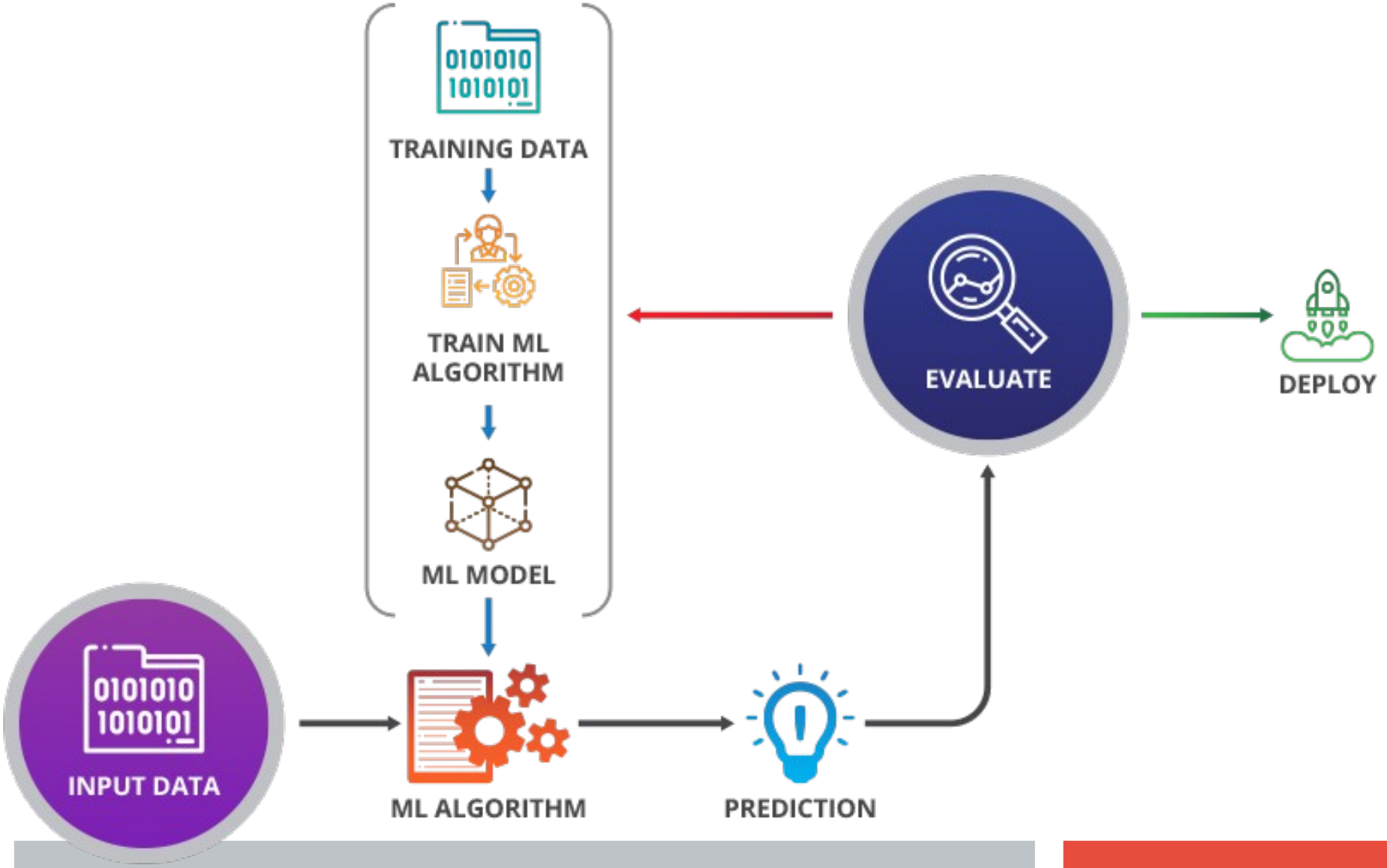


WAYS TO PROTECT AGAINST HACKERS MANUALLY

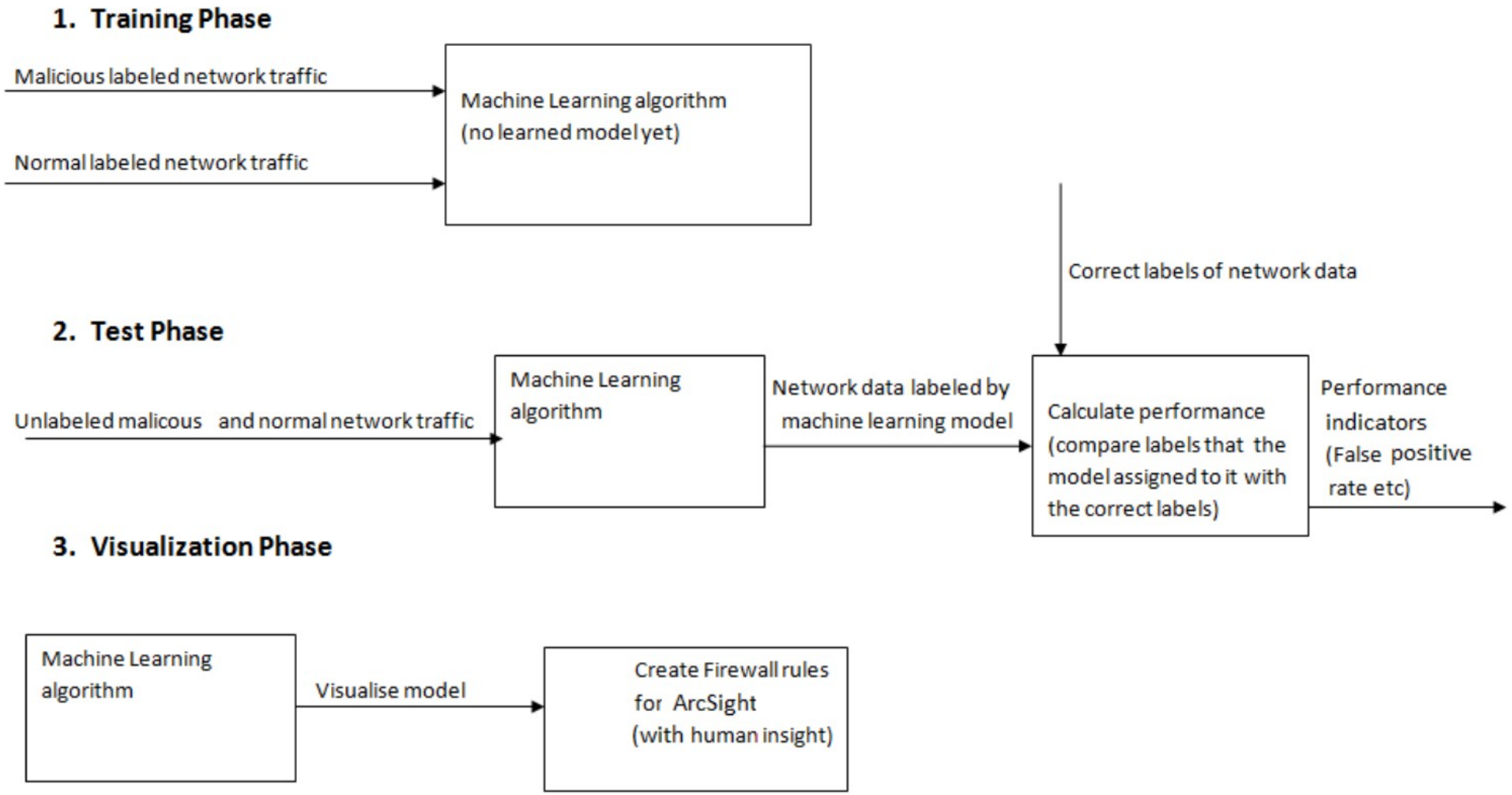
- Use a firewall,Vulnerability Assessment
- Install antivirus software
- Use complex passwords
- Keep your OS, apps and browser up to date
- Ignore spam
- Use encryption
- Back up your Data

But now we can see the Automatic Machine Learning Models to do the same.

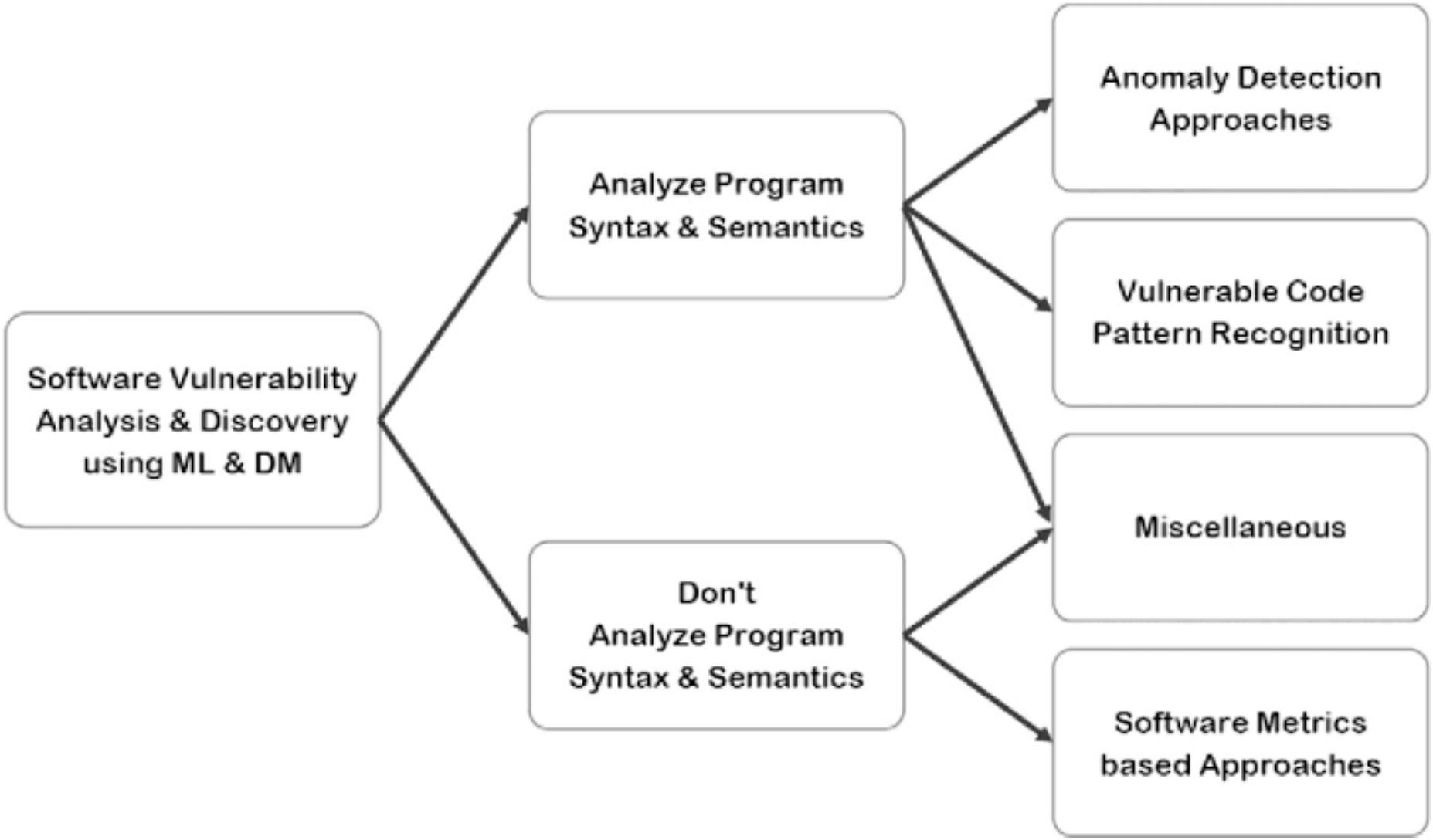
HOW MACHINE LEARNING WORKS



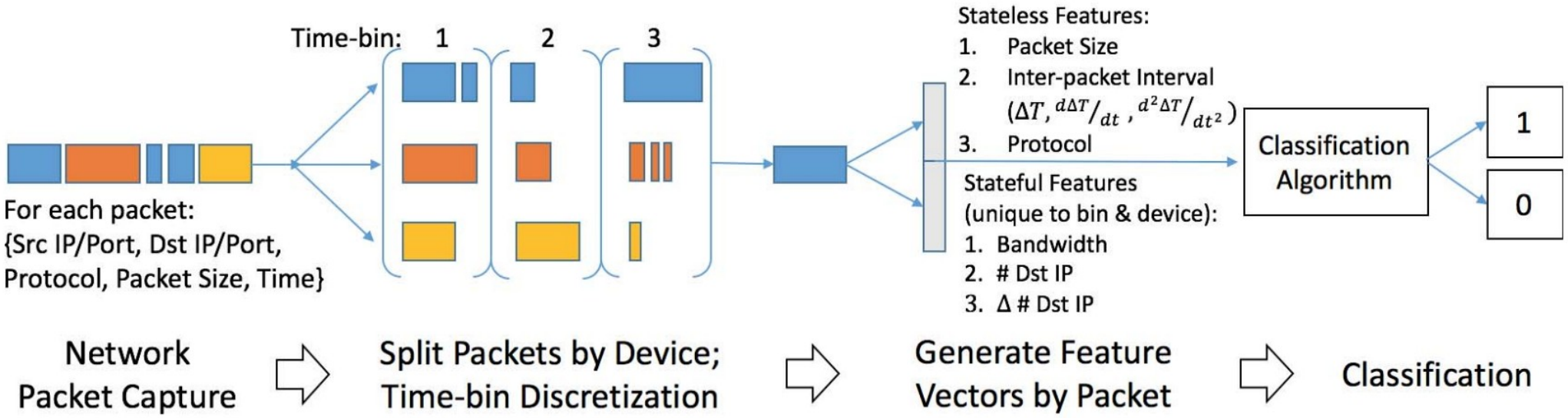
CREATING FIREWALL RULES USING ML



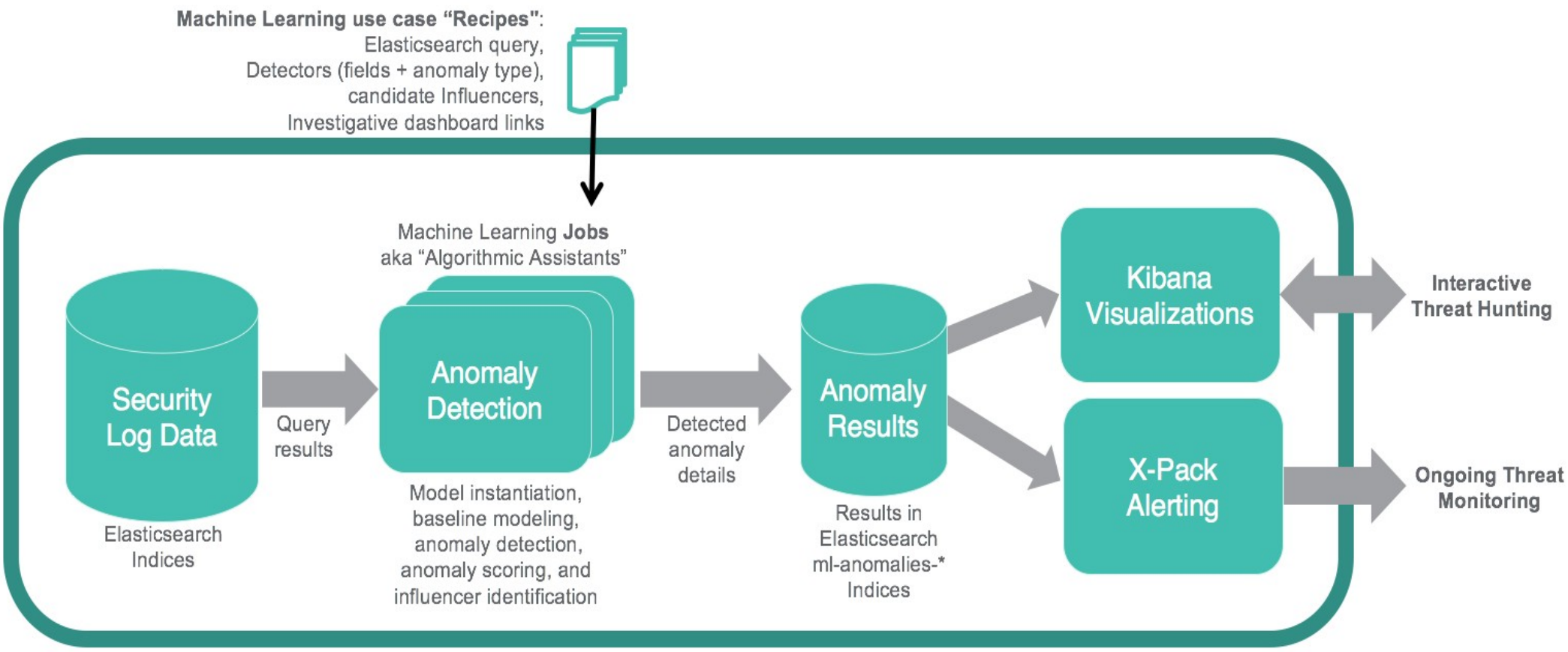
SOFTWARE VULNERABILITY



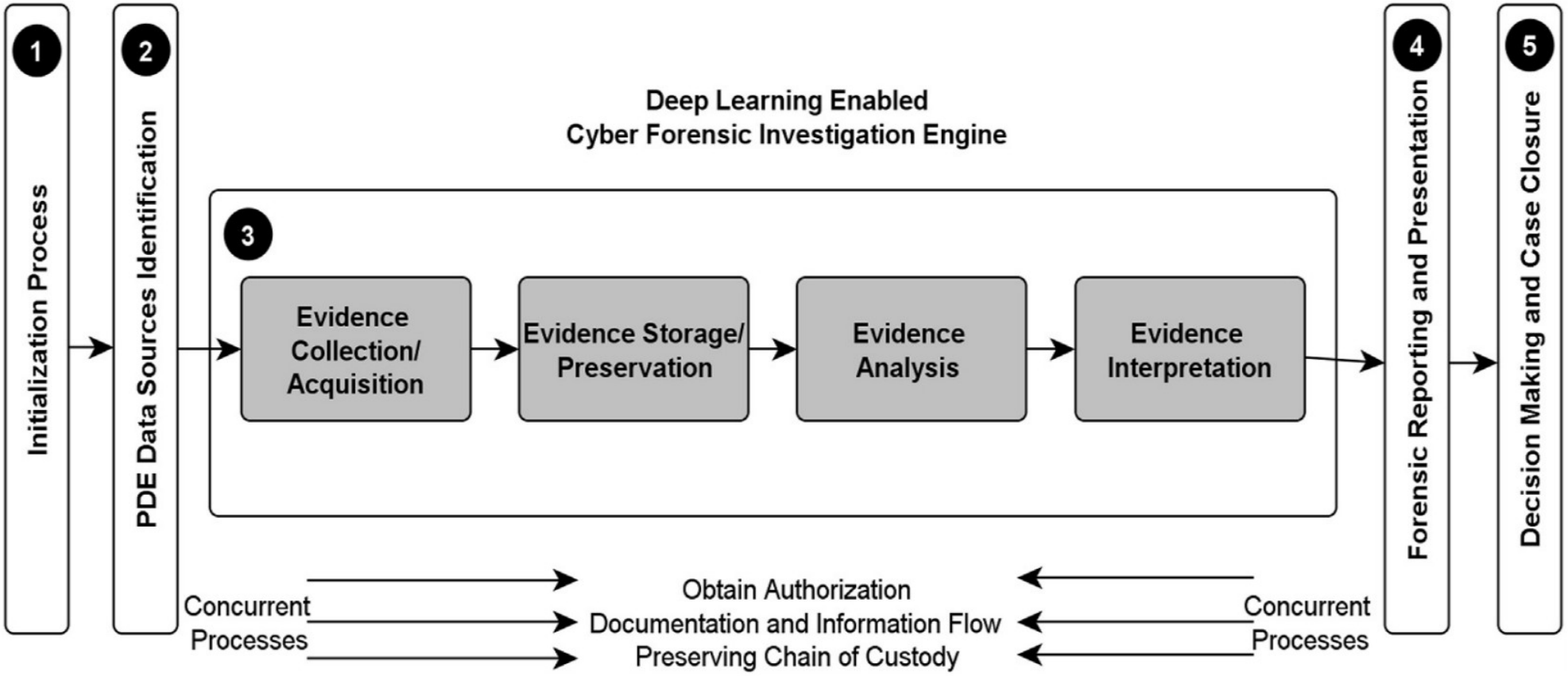
IOT DDOS DETECTION PIPELINE



THREAT DETECTION USING LOG FILES



DIGITAL FORENSIC ENGINE



PROBLEMS TO APPLY ML ON CYBER-WORLD

- Lack of Labeled Samples and Certainty in Ground Truth
- Imbalanced Data Sets
- Access to Data Sets
- Getting Bad Prediction
- Wrong Assumptions
- Bad Recommendation
- Needs a Very good Hardware Resources

SUMMARY

- Real Time Analysis
- More Effictive then Manual
- Less work more secure
- Hackers can also used to attack
- At present very few ML framework available in merket
- In future this may have a very good scope

REFERENCE

1. DeepLog: Anomaly Detection and Diagnosis from System Logsthrough Deep Learning by Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar

2. Anomalous Payload-Based Network Intrusion Detection by Ke WangSalvatore J. Stolfo

3. A state-of-the-art survey of malware detection approaches using data mining techniques by Alireza Souri,Rahil Hosseini

4. Machine Learning and Security by O'reilly

THANK YOU

sandipan@parrotsec.org