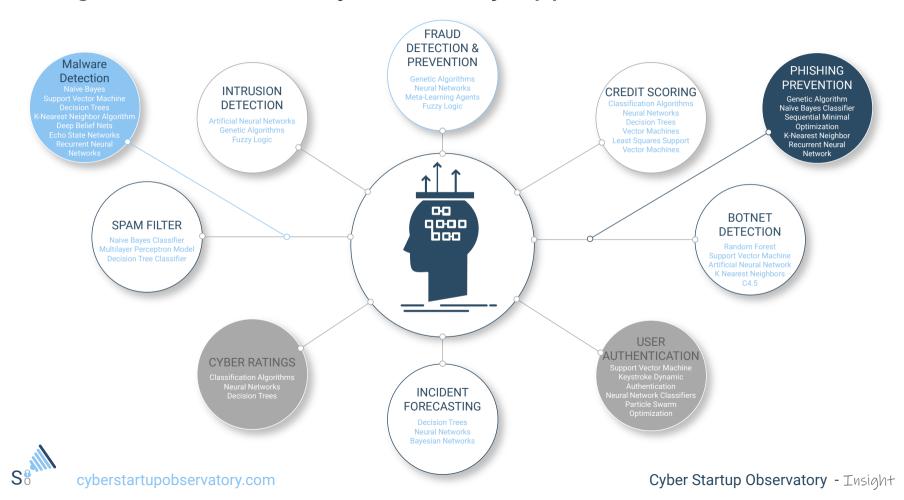
Al Algorithms Used in Cybersecurity Applications



Artificial Intelligence: Compliance and Regulatory Challenges



PRIVACY & CONFIDENTIALITY

- The expansion of AI has implications on personal privacy, which is a fundamental human right.
- Some of the information learned might be private or confidential even when the data mined to extract this insight might not be considered as PII or confidential.
- This might be particularly serious under regulations like GDPR.

2

ACCOUNTABILITY & LIABILITY

This is both a fascinating and extremely complex issue. Several questions arise:

- Who is going to be liable when autonomous decision-making, AI enabled, processes cause damage?
- Will sophisticated or autonomous algorithms be subject to traditional product liability legal frameworks?
- Is there a need to create a new treatment for "Thinking Algorithms"?
- Will it be needed to create a classification and specific treatment based on their level of autonomy?



GOVERNANCE

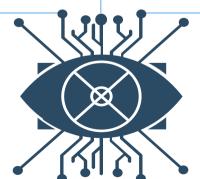
Al algorithms have common features that will complicate overall governance :

- · There are no one-size-fits-all solutions.
- Governance is going to have cross-border nature, requiring global dialogue and collaboration.
- The AI industry is evolving quickly. Governance and Regulatory initiatives are slow by nature.



BIAS & DISCRIMINATION

- The Al industry is fast-moving and largely unregulated.
- · Developers will need to avoid "Bias deep inside the code".
- Algorithms must not discriminate on grounds of age, race or gender.
- Ethical standards will need to be defined and enforced. This is not going to be an easy process for regulators.
- Bias and discrimination are going to be critical for compliance in Financial Services, Government Services and generally speaking in highly regulated industries.



5

ALGORITHMIC TRANSPARENCY

- If we do not know what an Algorithm is doing, we cannot hold it accountable.
- The transparency topic might be a serious issue in particular in regulated industries.
- This is especially problematic when implicating people, and it is not easy to address this problem as just because someone has access to the ML code, it does not always equal being able to explain how the software works.
- Transparency affects several dimensions, including:
- · Data and Algorithms used
- · Goals and Outcomes
- · Influence and potential manipulation



Major Applications of Machine Learning (ML) in Cybersecurity

WHERE IS ML APPLICABLE?

- Where we have lots of data either on the cloud or on the endpoint, IoT- IIoT, working on combination with big data and analytics
- To identify anomalies, suspicious or unusual behaviour
- Detect and correct known vulnerabilities and zero-day attacks
- When computer or machine time versus human time is a major requirement

INCIDENT RESPONSE & FORENSICS

- In the unfortunate case of an attack, an automated response in critical in order to minimize the impact, conduct forensics and to defend effectively
- From a defensive perspective we need to be able to respond in computer or machine time versus human time to stop some of the attacks
- Defense against intelligent cyber weapons can only be achieved by intelligent software
- The accuracy and effectiveness of the response to an attack could also be improved leveraging ML which is also quite import considering that cybersecurity has quite low fault tolerance as it only takes one vulnerability to be exploited in order to have a data breach

THREAT EXAMPLES

Specific threats that could be addressed with ML:

- · Spear Phishing
- Ransomware
- DDoS
- Watering Hole
- Webshell

- DNS Poisoning
- Port ScanningDefense against
- intelligent cyber weapons

FRAUD D

FRAUD DETECTION

- Machine Learning (ML) is increasingly being introduced to fight e-commerce fraudsters
- There is currently access to lots of information about suspect fraudsters, including their purchase activities and profile, online browsing activities, social networks and fake identification they submit to get tier orders approved
- The challenge is how we can make sense of this unstructured data and then make good approve / decline decisions for thousands of merchants in real-time

ENHANCE HUMAN ANALYSIS

- ML might help to address the acute problem of scarce and expensive expertise through resource optimization or increase in staff productivity
- Also a substantial reduction in false positive rates would positively impact cybersecurity operations and ML is very effective in achieving this goal
- We need to be cognizant that the widening cyber-security skills gap is seriously threatening companies and this serious issue needs to be addressed in terms of cyber risk exploited in order to have a data breach



