# Using Machine Learning for Cyber Threat Detection

We all live by rules, some rules are defined strictly and some loosely. There is new research in social psychology about how our world is wired by rule makers & rule breakers[1], including how all of us as people and communities are wired to follow some rules 'tightly', and some 'loosely'. Cybersecurity is eventually about people, and how some break rules (attackers) and others make rules (Cyber Warriors & products).

The cybersecurity effort at the very heart of it is a pattern recognition problem, trying to understand patterns of attacks in various ways and classifying them into benign (rule follower), malicious (rule breaker), or potentially requiring more investigation on precise intent. So, what is the role of Machine Learning (ML) in such pattern recognition problems?

As we will explore more below, machine learning is a technology built for pattern recognition on a large amount of data, especially patterns that are hard to uncover by writing signatures for, and hence ML plays quite an integral role in solving cybersecurity problems.

## Supervised vs. Unsupervised Learning: Two Fronts of Defense

All cybersecurity solutions are about learning from the past and current, and operationalizing that learning into the future protection. One way to do this is to learn and gain knowledge of exact patterns ('tight' rules of recognition) that define what is malicious, like hashes of malware files, domain names known to host malware or CnC sites, email addresses or domains used for phishing and spamming, strings inside executables or scripts that would potentially initiate unauthorized execution, etc.

In some of these cases, the amount of data that is known to be malicious (or not) is very large and/or dynamic with a substantial number of new samples added every day – this is the case, for example, for known malware files identified every day (order of a million new samples a day[2]). As one can see, identifying such files, creating signatures, and operationalizing them constantly is an intractable problem due to the scale and other issues.

To solve this problem in a tractable manner, a Supervised Machine Learning algorithm can create a model (that can be thought of as a learned rule that infers the likelihood of a sample being malware) based on known examples of benign-ware and malware. Apart from being able to classify known malware from benign samples, similar to a feed to signatures, it can also be predictive in its protection against malware files, i.e. identify previously unseen variants of malware.

Supervised ML usage for detecting malware files based on various parameters of the files (structure of file, content in file, use of different features in file formats, behavior of file when executed or opened in application) is now pervasive in the industry and has been proven to be quite successful in its coverage for detecting threats of the future. There are many other uses of Supervised ML, for example detecting if new domain names and certificates closely match known malware usage for such.

The other side of pattern recognition is when one where there are 'loose' rules of recognition, i.e., one can find a pattern that is not consistent in time and hence gives a start point of a

potential threat hunting and investigation into an event that might be malicious, and not detected by other techniques. Patterns of network activity vary for different types of computers used at different places in an enterprise and vary on days and times (weekday vs weekend for example).

To find inconsistency in network activity over time, Unsupervised Machine Learning algorithms can be used to create a baseline of network traffic activity for different types of assets and users and use that to find new or rare activity of some type that is an anomaly and deserves further investigation into whether it is a credible threat. Discovery of such anomalies is predictive of potential threats in an enterprise that might have gone undetected by all other technologies in place.

The use of Unsupervised ML to detect anomalies and hence threats is a newer use of ML algorithms in the industry and requires a threat hunting platform to enable an operator to use an anomaly for hunting and investigation of a credible threat. This is markedly different than the detection problem where there is higher confidence in determination of malicious intent. Anomalies without support from a threat hunting platform provide little value in threat detection and a high amount of false positive workload for operators. But anomalies in the hands of threat hunters with supporting investigation data can lead to advanced threat detection and potentially save on attacker dwell time and impact on an enterprise.

Figure 1. Different security functions in time & knowledge axes

## Operationalizing ML Models: Fidelis Network

Fidelis Network uses both Supervised & Unsupervised ML algorithms (in addition to signatures, rules, analytics, IOCs) to create future detections (Proactive Defense) and anomalies that warrant investigations (Predictive Analysis using ML) as shown in Figure 1. The role of a Network Traffic Analysis product like Fidelis Network is to detect the known threats and to help hunt the unknown threats and facilitate further investigation, in both past data and in real-time (future). Machine Learning algorithms play a role in both aspects of detection, threat hunting and investigation.

Unsupervised Machine Learning based behavioral anomaly detection can be an effective defense against advanced threats, especially when combined with information on user accounts, assets,

and cyber terrain. Fidelis Network uses this approach to detect suspicious activities related to lateral movement using stolen credentials, CnC activity, and data theft (that can be possibly from an insider theft).

## References


1. ^ Michele Gelfand, “Rule Makers, Rule Breakers: How Tight and Loose Cultures Wire Our World”, 2018. More information available at https://www.michelegelfand.com/rule-makers-rule-breakers.
2. ^AV-Test, “Malware Statistics & Trends”, May 2020. Available from: https://www.av-test.org/en/statistics/malware/