Questions 03-26-2018

Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey:

This article concludes that much improvement can be had by employing updated and accurate training data as well as using an ensemble or multi-part approach to classifiers. With this being the case, what methods of updating the training can we think of? Are there methods of updating the training data accurately and autonomously that we can contemplate? On top of this, can we think of efficient manners of ensemble classification as changes and developments in the field arise?

Lambda Architecture for Cost-effective Batch and Speed Big Data processing:

This article discusses a proof-of-concept of a cost-effective model for data processing. Specifically, it discusses one using a lambda architecture on Amazon Web Services. How might a cost-effective architecture for data processing help with big data processing in regards to cyber security? Do we think this is a way to solve specific problems in cyber security, and if so, which ones?