A framework based on dynamic algorithm configuration and incremental learning to protect UEBA algorithms from conceptual drift, cyber deception techniques and model-poisoning

Thomas Anglade[1], Thierry Berthier [2]

[1]ITrust (tanglade@itrust.fr)
[2]Limoges University, Limoges, France (thierry.berthier@unilim.fr)

Abstract.

Over the last years, the progresses made regarding unsupervised machine learning and behavioral analysis contributed to the development of advanced UEBA-based network intrusion detection systems (IDS). These systems allow private and public companies to adapt themselves to the growing complexity of cyber-attacks and APTs. Nevertheless, scientific and operational works regarding UEBA IDS tend to agree upon the fact that these models emphasize several weaknesses: difficulty to integrate the evolution of behavior through time (also known as "concept drift"), vulnerabilities to progressive multi-stage attacks, model poisoning, and deceptive adversarial reinforcement-based attacks.
This paper completes our work presented at the C&ESAR 2019 conference and offers tools to strengthen UEBA-based defensive frameworks by addressing these vulnerabilities, based on the following emerging machine learning tools: incremental learning, dynamic algorithm configuration and reinforcement learning. Our method allows to optimize the model's meta-parameters and to recalibrate the model's parameters using fresh data, threat intelligence and cyber analysts' feedbacks on anomalies previously generated by the algorithm.

Keywords:
cybersecurity, UEBA, deception, incremental learning, dynamic algorithmic configuration, reinforcement learning, model poisoning, conceptual drift