SENTRY: Semi-Supervised Efficiency-First Threat Recognition System

Al-Shami, Humam (School: Arkansas Connections Academy)
Alroobi, Mohammed (School: Arkansas Connections Academy)

As cyber-attacks become increasingly common (72% increase from 2021), and as losses from cybercrime grow each year ($10.5 trillion by 2025), it is more important than ever for organizations to protect their digital assets. Yet, the high costs for Cloud-Based Endpoint Detection & Response solutions pose a significant barrier to smaller-sized organizations and educational institutions due to the complexity of the Machine Learning techniques utilized. While rule-based methods are more affordable alternatives, they falter when compared to Machine-Learning EDR solutions due to their inability to detect new threats with unknown signatures. Finally, the lack of open-source labelled data for newer attacks makes it difficult to maintain a robust solution. To address these challenges, we propose a Semi-Supervised Machine Learning approach that would allow for a dynamic solution that can easily adapt to new threats with minimal maintenance, can accurately recognize threats, and prioritizes efficiency. Through our approach, we were able train a Seeded K-means model using Windows EVTX Logs, obtaining inference speeds of less than 0.1 seconds using less than 250MB of RAM. We achieved a binary threat-detection accuracy of 99% and a multi-class accuracy of 83% using 8 MITRE ATT&CK TTPs, outperforming current solutions in our testing.

Awards Won: