The Efficiency of machine learning Techniques in minimizing Dwell Time of Cyberattacks

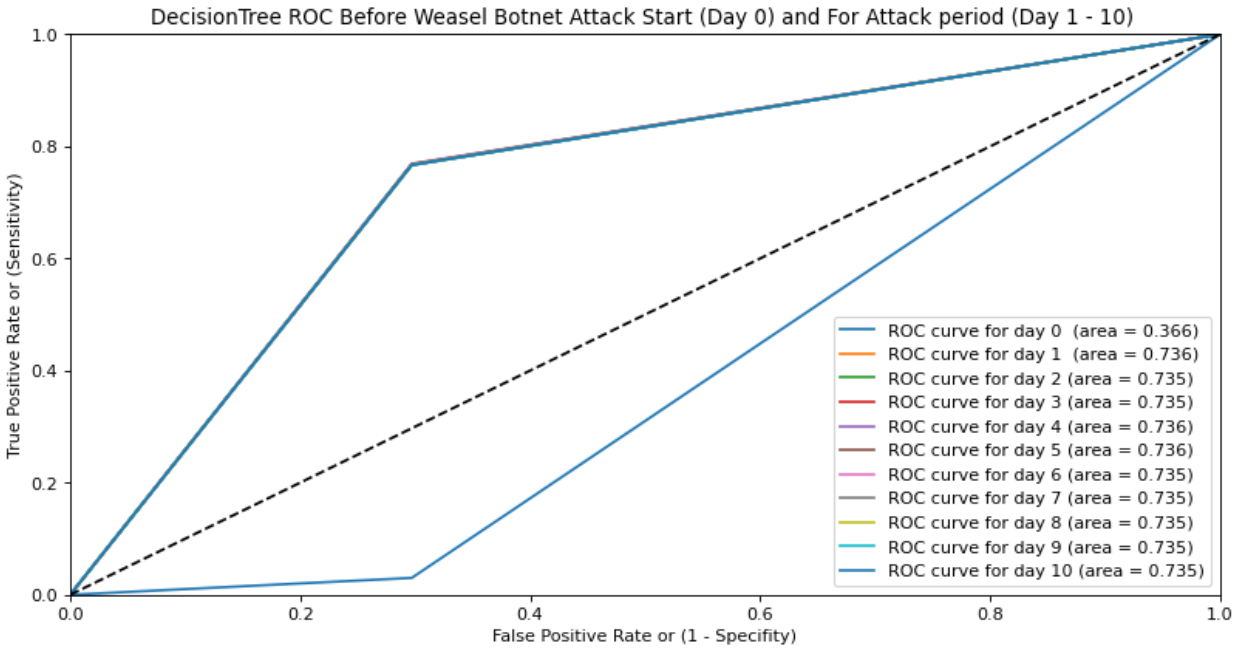
Minimum Viable Product (MVP):

Cyberattacks Dwell Time is the time between when a compromise first occurs and when it is detected. The goal of this project to detect the cyberattack as early as possible to eventually minimize Cyberattack Dwell Time.

The initial step to answer project question I extracted two datasets one for training to check the model validation. The second dataset is used to evaluate the model generalization for unseen data.

Instead of having the security operation center (SOC) analyst fighting false positive for log time without detecting the existence of cyberattack, I produce a novel methodology (to the best of my knowledge) based on Receiver Operating Characteristic (ROC) as heuristic to alert the (SOC) analyst early for the cyberattack once the auc exceed 0.5 as shown in below figure

MVP



The initial result is optimistic, however once auc exceed 0.5 in day one of cyberattack it is improved slightly on the rest period of cyberattack which I will try to improve.