

Ransomware Anomaly Detection

Students: Alwahab Mohammad

Mentor: Mike East, Kaseya; Carl Banzhof, RocketCyber

Instructor/Faculty: Dr. Masoud Sadjadi, Florida International University

PROBLEM

Technology as of now is growing rapidly along side with the intricacies of cyber attacks, including ransomware attacks.

This calls for the need for increased. Ransomware has been prominent for the last few decades, and security has been updated to adapt and prevent these attacks. The problem can be detecting these ransomware attacks may be too difficult and may need quick detections of anomalies and ransomware attacks.

Machine Learning will be the foundational approach to detect anomalies within the system Windows logs to detect ransomware.

CURRENT SYSTEM

The Windows OS saves thousands of event logs in the computer stating the actions the system takes. The current system uses Sysmon archive files, extracted with Python-based coding, and trains the machine with Machine Learning. This trains the machine of what is normal, and this is compared to new event logs to determine dissimilarity among the events.

Streamlit is used to visualize the data the machine returns onto charts and is then used to determine if an anomaly is found.

REQUIREMENTS

Windows 10 OS

Python 3.10

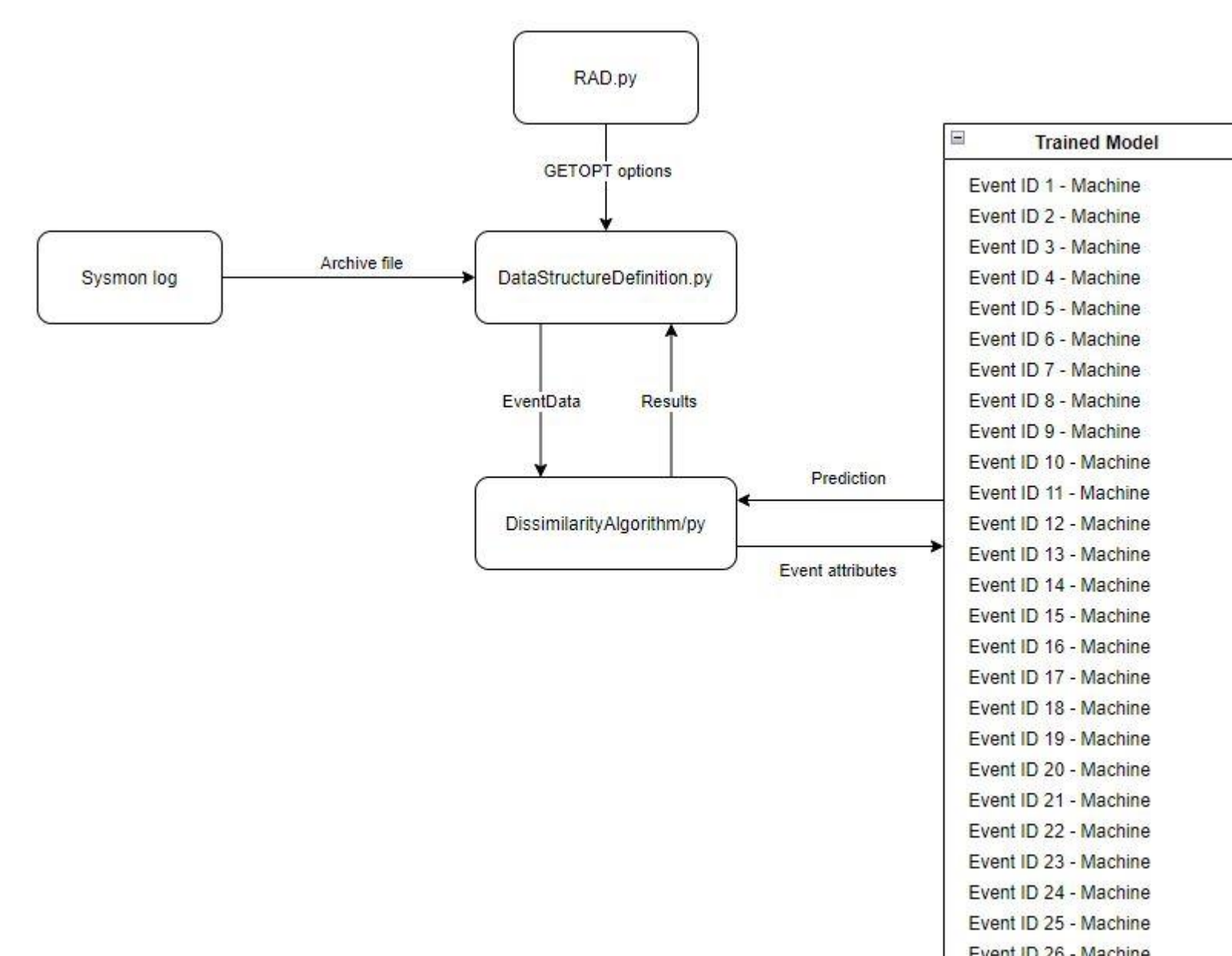
GitHub for Version Control

Windows Sysmon logging tool

Sysmon Simulator for testing

Streamlit packages and internet

SYSTEM DESIGN

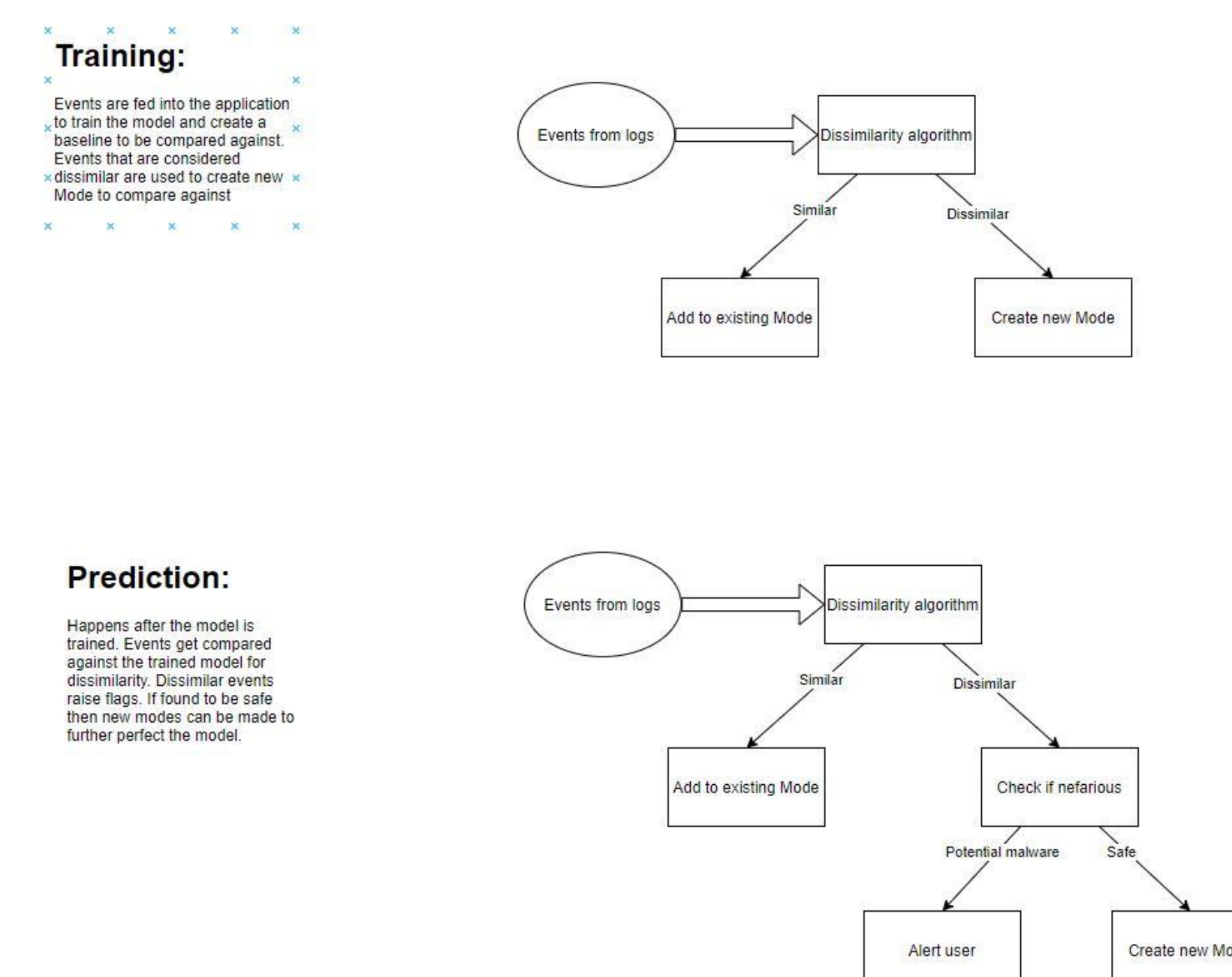


VERIFICATION

Sysmon Simulator is an application that is used to mimic ransomware events, which are also recorded in the Sysmon log files. This was used to test the legitimacy of the application.

The application found anomalies from the Sysmon Simulator with a success rate of 75% alongside with less than 1% of the sample being false positives

OBJECT DESIGN



SUMMARY

What I contributed to this project:

Researched Sysmon Event logs and identified key attributes to parse.

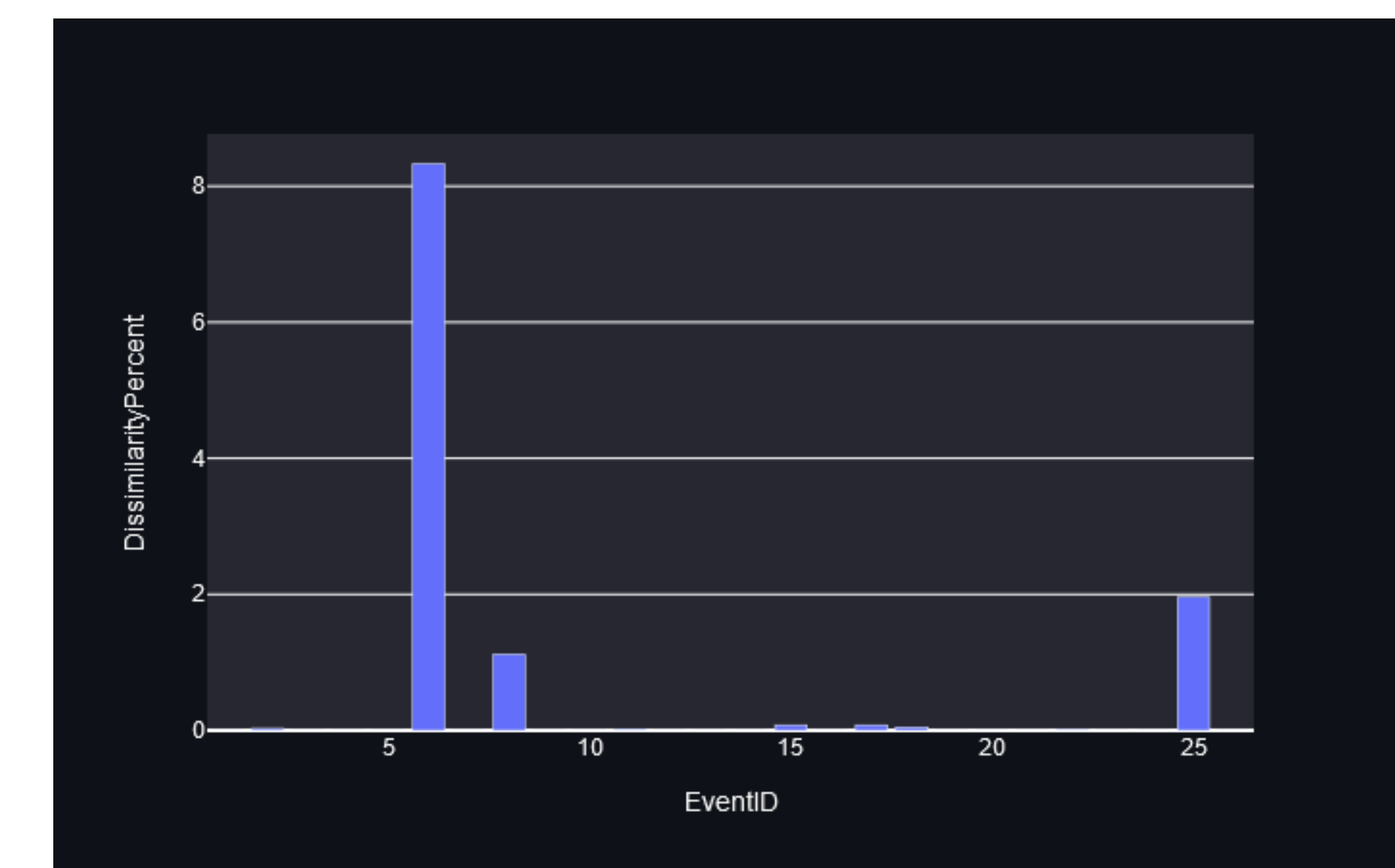
Research into Machine Learning Techniques on Supervised learning.

Researched Data mining techniques for outlier detection, finding statistical methods: parametric and nonparametric

Developed and implemented Streamlit web application to visualize data using streamlit, pandas, and plotly packages

IMPLEMENTATION

After running the machine using Python, Machine Learning training methods, and data mining techniques (k-means clustering), the machine returns training data results. The results would display the Event IDs, Modes, number of Events Trained, and Dissimilarity Percent. This data is plotted on multiple charts/graphs using Streamlit for visualization. An example bar chart of Event IDs vs Dissimilarity Percent is shown:



REFERENCES

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

<https://github.com/ScarredMonk/SysmonSimulator>

<https://docs.streamlit.io/>

ACKNOWLEDGEMENT

We thank Professor Masoud Sadjadi, and Mike East and for their assistance and mentorship that we received throughout the capstone 2 design project.